United States Trustees Program

Privacy Impact Assessment
for the
Means Test Review Management System (MTR)

Issued by:
Larry Wahlquist, Privacy Point of Contact

Reviewed by: Vance E. Hitch, Chief Information Officer, Department of Justice

Approved by: Nancy C. Libin, Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: March 24, 2011

(February 2011 DOJ PIA Form)

Introduction

The United States Trustee Program (USTP) is a component of the Department of Justice (DOJ) that seeks to promote the efficiency and protect the integrity of the Federal bankruptcy system. The USTP monitors the conduct of bankruptcy debtors, parties in interest, and private estate trustees, oversees related administrative functions, and acts to ensure compliance with applicable laws and procedures. It also identifies and helps investigate bankruptcy fraud and abuse in coordination with United States Attorneys, the Federal Bureau of Investigation, and other law enforcement agencies.

The Means Test Review Management System (MTR) was developed to support the USTP with the review of the bankruptcy means test form required under the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA), 119 Stat. 23, April 20, 2005. The BAPCPA gives the USTP responsibilities in a number of areas, one of which is implementing the "means test" to determine whether a debtor is eligible for chapter 7 (liquidation) or must file under chapter 13 (wage-earner repayment plan). The means test is the basis for determining whether a presumption of abuse applies in those cases where a debtor's current monthly income exceeds the state's median income for a household of the same size as the debtor's. As of October 17, 2005, certain debtors are required to file a means test form along with their petition and schedules within 45 days of filing for bankruptcy.

The MTR System tracks the filing of all chapter 7 cases and facilitates the review of the means test form, petition and schedules to verify the results. In addition, the MTR System tracks due dates for required USTP Presumption of Abuse Statements and related motions.

Data received from the courts for bankruptcy cases is loaded into the USTP Automated Case Management System (ACMS). Relevant case data is then also copied to the MTR System after it is loaded into ACMS. This process ensures case data is current and accurate and streamlines data entry (no need to re-enter the data again). Basic case information, case number, debtor name, address, chapter, debtor attorney name, and judge name is populated from ACMS to MTR for the cases requiring a MTR review. In addition, the status of any USTP motions relating to the means test review are listed in the MTR system. So if a USTP Statement of Presumed Abuse is filed with the court, this event is loaded into ACMS and "shared" with the MTR system. Most case files do not contain social security numbers (SSNs) or other personal information; however, there are a few instances where social security numbers are present in the Portable Document Format (PDF) images filed with the court by the debtor. The PDFs containing the means test form, petition and schedules are downloaded daily from the courts and included in the MTR system.

The MTR functions include searching for cases, reviewing a list of pending cases, reviewing the status of the case review, reviewing the individual data fields of the means test form, and producing reports.

Section 1.0
The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

MTR stores only basic bankruptcy case information: the case number, debtor name, address, filing chapter, debtor attorney name, trustee name, judge name and any assigned USTP staff names. In addition, PDF files of the petition, schedules, means test form and statement of financial affairs are viewable via the MTR System for all open chapter 7 cases along with any notes to the files submitted by USTP staff. SSNs are generally not maintained in MTR; however there are a few instances where SSNs are present in the PDF images filed with the court by the debtor.

1.2 From whom is the information collected?

Information is obtained from ACMS, which receives information directly from the bankruptcy courts as explained in the ACMS Privacy Impact Assessment. In addition, users may manually enter notes. The notes generally indicate the status of the review, such as waiting on additional documentation from the debtor or debtor's attorney.

Section 2.0
The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

The information collected by MTR is needed to track the filing of all chapter 7 cases to facilitate USTP review of the monthly income data provided on debtors' schedules and Means Test form in order to verify the results. In addition, the MTR System tracks associated due dates for required USTP Presumption of Abuse Statements and related motions required under the BAPCPA.

The information collected also supports the search and reporting functions that allow USTP to track the status of all chapter 7 cases for an office or region. These reports aid offices

and regions with managing upcoming filing deadlines, as well as identifying legal issues and trends requiring further analysis.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

The USTP was established by the Bankruptcy Reform Act of 1978 (11 U.S.C. § 101, et seq.) as a pilot effort encompassing 18 districts. It was expanded to 21 Regions nationwide, covering all Federal judicial districts except Alabama and North Carolina, by enactment of the Bankruptcy Judges, U.S. Trustees, & Family Farmer Bankruptcy Act of 1986 (Pub. L. 99-554, 100 Stat. 3088, reprinted in part at 28 U.S.C. § 581, note).

The primary role of the USTP is to serve as the "watchdog over the bankruptcy process."[1] As stated in the USTP Mission Statement:

> The USTP Mission is to promote integrity and efficiency in the nation's bankruptcy system by enforcing bankruptcy laws, providing oversight of private trustees, and maintaining operational excellence.

www.justice.gov/ust/eo/ust_org/mission.htm.

The Bankruptcy Code grants to the USTP the authority to supervise the administration of bankruptcy cases. The USTP's Systems of Records Notice (SORN), 71 Fed. Reg. 59,818 (Oct.11, 2006) specifies the information that will be collected by the USTP, including personally identifiable information (PII).

The Administrative Office of the United States Courts (AOUSC) provided the USTP with daily data files of bankruptcy case opening and closing information for many years without a formal agreement. In 2003, the AOUSC enhanced the Case Management/Electronic Case Files (CM/ECF) Program to include a Data Exchange module (DXTR) specifically to provide daily data files of case opening, closing, and docket events and in 2005, the AOUSC turned on the feature to provide Portable Document Formats (PDFs) daily, as well. In 2009, the AOUSC and the Executive Office for United States Trustees entered into a formal Memorandum of Understanding (MOU) detailing the terms and conditions concerning this transfer of information.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

Potential privacy risks include unauthorized access to and use of the data, inadvertent disclosure of the data, and inaccurate data. The risk of inaccurate data is minimized, in part, by

[1] House Report No. 989, 95th Cong., 2d. Sess., at 88 (reprinted in 1978 U.S.C.C.A.N. at 5787, 5963, 6049)

the fact that much of the bankruptcy case information collected in MTR is received directly from the court via ACMS and the DXTR download. Also, MTR collects the minimum amount of personally identifiable information (PII) necessary to achieve the purposes of the system. To mitigate the privacy risks, MTR contains safeguards against disclosure of information by limiting access to MTR to role-based access and periodically auditing such access. (See discussion in Section 8.9.) In addition, the USTP has provided guidance to all staff on how to safeguard MTR data, both internally and when transferring such data outside of the USTP. As discussed below in Section 3.3, safeguards are in place to ensure that data is accurate and no action is taken against an individual based solely on information in MTR.

Section 3.0
Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

The MTR uses include searching for cases, reviewing a list of pending cases, reviewing the status of the case review, reviewing the individual data fields of the means test, and producing reports.

The information collected and maintained by MTR will be accessed by the USTP staff. Information that is received directly from the AOUSC via ACMS and the DXTR download will generally not be shared with other entities, unless the information qualifies as a necessary report as described in the MOU. Other case information that is not derived from the DXTR download may be shared, as appropriate, with law enforcement agencies. This information will only be shared with another DOJ component or law enforcement entity that has a demonstrated need for the information in the performance of its official duties. The routine uses that delineate the uses of this information are specifically covered under the USTP's SORN as published in the Federal Register on October 11, 2006 at 71 Fed. Reg. 59,818.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

MTR provides search and reporting functions to track the status of all chapter 7 cases for an office or region. These reports aid offices and regions with managing upcoming filing deadlines, as well as identifying legal issues and trends requiring further analysis. However,

MTR is not engaged in data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53.

3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

Much of the bankruptcy case information in MTR comes from ACMS. The USTP established internal minimum ACMS standards in 1992 and updated them in 2006. ACMS data is reviewed daily and compared against the courts systems, as appropriate. In addition, various quality control reports are run to ensure all requisite case data has been received from the bankruptcy courts and appears in ACMS.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

A records retention schedule for MTR has been reviewed and approved by the National Archives and Records Administration (NARA). The retention period for data in the system is 20 years.

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Access to the system is role-based. Based on the user's role in the case review process, a comparable role is granted to the end user at the application and database level. A user is granted access after the user has received the requisite security clearance and the proper request form has been approved by the appropriate management and submitted for processing. In addition, guidance is provided on how to safeguard Limited Official Use data.

Section 4.0
Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

Information that is received directly from the AOUSC via ACMS and the DXTR download will generally not be shared with other components, unless the information qualifies as a necessary report as described in the MOU. Other case information that is not derived from the DXTR download may be shared, as appropriate, with the US Attorney's Office, Federal Bureau of Investigation, Civil Division Appellate Section or Criminal Division. This information will only be shared with another DOJ component that has a demonstrated need for the information in the performance of its official duties.

4.2 For each recipient component or office, what information is shared and for what purpose?

The bankruptcy case information described in Section 1.1 may be shared as it relates to a bankruptcy investigation. The purpose of the sharing would be for official law enforcement purposes, such as referring a case to the appropriate United States Attorney's Office for further investigation. The purpose for sharing information is identified in the USTP's SORN at 71 Fed. Reg. 59,818 (Oct. 11, 2006).

4.3 How is the information transmitted or disclosed?

This information is relayed via email, facsimile, or hard copy. If sent via hard copy, the package would be double-sealed and hand-delivered, where possible, or sent via Federal Express and tracked. Information would be sent to established contacts within investigation offices.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

The potential privacy risk with sharing of information internally is the increased risk of unauthorized use or disclosure of MTR data. As stated above in Section 2.3, the risk is minimized because most of the information collected in MTR is obtained from the bankruptcy courts. With the exception of the full social security number, which is not routinely kept in MTR, most of the information is available to the public via the courts' PACER system. During the system development process, USTP was sensitive to only collecting the minimum amount of PII data that was necessary to perform its review. Therefore, only case name, case number, debtor name, debtor address, filing chapter, names of the attorney, trustee and judge, and USTP staff assigned are captured in the MTR system. In order to minimize the risk of inadvertent disclosure of any PII data, access to the system is limited. All logins and access are tracked within the database. In addition, the USTP has provided guidance to all staff on how to safeguard the transfer of Limited Official Use data.

The USTP Security Features User's Guide provides details on how to handle and safeguard sensitive information. PII stored on any removable media (CD/DVD, USB drive, floppy disk, etc.) that leaves DOJ facilities requires additional protection and must be encrypted with USTP-approved encryption software.

The risk of unauthorized use is minimized by not allowing other DOJ components direct access to the information and only sharing information when there is a legitimate need to know.

Section 5.0
External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DOJ which includes foreign, Federal, state and local government, and the private sector.

5.1 With which external (non-DOJ) recipient(s) is the information shared?

Information that is received directly from the AOUSC via ACMS and the DXTR download will generally not be shared with external recipients, other than trustees, unless the information qualifies as a necessary report as described in the MOU. The sharing of information is accomplished through the routine uses specified under the USTP's SORN as published in the Federal Register on October 11, 2006 at 71 Fed. Reg. 59,818.

5.2 What information is shared and for what purpose?

See 4.2.

5.3 How is the information transmitted or disclosed?

See 4.3.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

External users are notified if the data being provided contains Limited Office Use data. Contractors are required to sign non-disclosure and confidentiality agreements for access to USTP data.

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

External users (non-USTP) are not given system access. Therefore, no specific training is provided.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

No, audits are not performed on the recipients' use of bankruptcy case data. However, bankruptcy trustee operations are audited to ensure they are compliant with USTP policy and have appropriately secured systems.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

The privacy risk with sharing information externally is the increased risk of unauthorized use or disclosure of MTR data. Other entities are not given direct access to the MTR system, and information is only shared when there is a legitimate need to know and such sharing is covered by a routine use or other provision of the Privacy Act. To reduce the risk of inadvertent disclosure when transmitting data, the USTP staff has been provided guidance on how to safeguard the transfer of Limited Official Use data. External users are also notified if the data being provided contains Limited Office Use data.

Section 6.0
Notice

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

A USTP SORN that covers the collection of information contained in the system was published in the Federal Register, 71 Fed. Reg. 58, 818, (Oct. 11, 2006),. Because the

information collected in this system is originally collected by the bankruptcy court, no notice other than the SORN is given to individuals before their information is entered into MTR. 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)."

6.2 Do individuals have an opportunity and/or right to decline to provide information?

No.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

No.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Because a Privacy Act SORN that covers the collection of information has been published in the Federal Register, and because the bankruptcy court in its instructions discloses that most of the information submitted in a petition will be public, the risk that an individual would provide information without knowledgeable consent is mitigated. The SORN provides the individual with transparency concerning the USTP's collection, use, and maintenance of the data.

Section 7.0
Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Individuals can make a request for access to or amendment of their records under the

Privacy Act, 5 U.S.C § 552a.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

Notice of individuals' rights under the Privacy Act is given through publication in the Federal Register of a SORN (71 Fed. Reg. 59,818 (Oct. 11, 2006)), and in DOJ regulations describing the procedures for making access/amendment requests. 28 C.F.R. § 16.40 et seq.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

No.

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

See the procedures discussed in Section 7.1. Additionally, if an individual exhausts his or her administrative remedies under the procedures in Section 7.1, the individual can file a lawsuit under the Privacy Act. No action will be taken against an individual solely in reliance on information in MTR.

Section 8.0
Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system?

Paralegals, analysts, attorneys, clerks and managers have access to MTR. The system is available to designated users at all USTP offices; however, access to information maintained by the system is restricted by system permission controls to only allow users to see information that they are entitled to see.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Yes. Contractors provide development and database support.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. USTP users are granted access to those case records managed by their office or region. Based on a user's role in the region, they may have access only at the office level or at the regional level. A few members of the Executive Office staff have access to all records.

8.4 What procedures are in place to determine which users may access the system and are they documented?

Please refer to Section 3.5. The MTR system is certified and accredited per DOJ requirements which include parameters on password expirations, account locking after a set amount of failed access attempts, and the auditing of event logs.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Individuals have specific roles that limit them to the data they enter or have specific rights to address as defined in the procedures. Actual assignments of roles and rules are established as defined in Section 3.5 for obtaining an account. The procedures for creating and maintaining system access are audited regularly and are part of the annual Federal Information and Security Management Act (FISMA) audit review process. Auditing and system log review are on-going activities. Additionally, database and system audits are conducted regularly to check for vulnerabilities, weak passwords, undocumented system changes, and policy deviations. Account activity is monitored for inactivity and other anomalies.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

There are roles and views defined to limit data access. Changes to these roles and permissions are captured in the system audit log and maintained on a separate logging server. All logins and access are tracked. Annual security training and the Rules of Behavior Certifications are required, which reinforce the rights and restrictions of system access.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

All employees are required to complete online information systems security training as part of annual training for DOJ employees. A certificate of completion is logged for employees after successful completion of the training. Also, new employees receive training on the use of this particular system before they are granted access to the system.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. The last Certification & Accreditation was completed in February 2009.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Because the data contains personal information, ensuring adequate security is critical. There is a clear separation of duties to prevent any one person from having sufficient access to allow inappropriate access or to work around the controls in place. The possibility of users or administrators being able to access information inappropriately has been addressed by having forced system and audit logs copied in real time to a secured logging server where the data is reviewed daily for anomalies. If logs do not arrive as expected, alerts are generated. The intrusion detection systems are monitored for unusual traffic, especially traffic going to the Internet. Training and reminding employees of their responsibilities, and the ability to track system usage in the event wrongdoing is discovered, helps mitigate this risk.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

Yes. In accordance with the Information Technology Management Reform Act of 1996 and the "best practices" prescribed by the Government Accountability Office and the Office of Management and Budget, the system has been developed in phases. Also, prior to each phase, the system developer engages in the gathering of functional requirements and tasks the developer of each phase to compare technologies in order to identify solutions that best incorporate the latest information system security controls required by FISMA.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

As part of the System Development Life Cycle (SDLC) process, data integrity, privacy and security were reviewed. The SDLC process requires a security review as well as

configuration and data management validation. Data integrity is partially covered by legal processes for collecting data and largely controlled by actual field parameters and data integrity checks. Since the data is Sensitive But Unclassified , privacy is assured by many system access limits and controls. Security is reviewed at all stages of the systems development life cycle in terms of security checklists and scans to ensure any design is FISMA-compliant and documented. These requirements are part of the system design documentation and it cannot be promoted during development if these steps are not addressed.

9.3 What design choices were made to enhance privacy?

Due to the sensitive nature of the information captured, a number of design choices were made to protect the data. The data libraries and programs are accessed by special purpose limited applications to ensure that users only have access to data on a need to know basis. A number of roles were designed to ensure that only the certain subsets of data could be viewed. Logs of user activity are in place as well as careful consideration of the client's interaction with the application further limiting potential user threat to the system.

Conclusion

In order for the USTP to fulfill its mission, it is critical that the USTP continue to receive the relevant bankruptcy case information, including personal identifiers, in a timely and expeditious manner to accomplish its mission. Without this information, the USTP would be unable to fulfill its statutory requirements. USTP will monitor the conduct of parties and take action to ensure compliance with applicable laws and procedures; identify and investigate bankruptcy fraud and abuse; and oversee administrative functions in bankruptcy cases. The USTP reviewing officials conclude that substantial measures are in place to protect the PII collected and proper education has been and will continue to be provided to ensure this data is treated as Limited Official Use by all USTP staff, contractor staff, and private trustees.