Privacy Impact Assessment
for the

Debtor Audit System (DAS)

[Short Form]

United States Trustee Program

March 19, 2007

Contact Point
Monique K. Bourque
Chief Information Officer
United States Trustee Program
(202) 353-3548

Reviewing Official
Jane C. Horvath
Chief Privacy Officer and Civil Liberties Officer
Department of Justice
(202) 514-0049

Introduction

The Debtor Audit Management System (DAS) was developed in FY 2006 for deployment in early FY 2007. This new system will manage the selection of cases for the random and non-random audits required under the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA) to be implemented as of October 20, 2006. The new system will also facilitate the audit assignment process, tracking the progress/results of the audits as well as the management of the payment of the outside auditors. The DAS shares data with the USTP Case Management System (ACMS) to ensure case data is current and accurate and to streamline data entry.

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?

The Debtor Audit System (DAS) shares data with the USTP Case Management System (ACMS) to ensure case data is current and accurate and to streamline data entry. Basic case information, case number, debtor name, debtor social security number, address, chapter, and debtor attorney name/address are shared between ACMS and DAS. In addition, results of an audit (full report is included as a PDF), information regarding the contractors performing the audits (names of the points of contact, mailing address, phone and fax numbers, contractor website, DUNS No., Tax ID number and purchase order info) along with payment status of audits submitted by contractors are captured in DAS.

1.2 From whom is the information collected?

The information is originally collected from individuals who have filed for bankruptcy, and the information appears in court filings in their bankruptcy cases. The bankruptcy case information contained in ACMS is primarily obtained directly from the U.S. Bankruptcy Courts either through a daily data file or manually entered from documents either filed with the courts or generated to support the case by the appointed trustee. The court data is downloaded daily from the U.S. Bankruptcy Courts to the USTP system via a secured (HTTPS) connection utilizing the existing Department Internet connection. The relevant case information is then shared with DAS. The results of the audit performed by the independent auditor are keyed into the DAS by

Program staff. In addition, pertinent contact and contract information is collected from the vendors who have contracted with the department to perform the debtor audits.

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?

Under the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA), the USTP is required to conduct random and non-random audits. The Debtor Audit System was developed to facilitate the selection and assignment process, track the status and results, and collect information to assist with further civil or criminal enforcement actions as well as assist with the compilation of data necessary to conduct the annual report to Congress.

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 Debtor Audit System will manage the selection of cases for the random and non-random audits required under BAPCPA. DAS will also facilitate the audit assignment process, tracking the progress/results of the audits as well as the management of the payment of the outside auditors. The DAS shares data with the USTP Case Management System (ACMS) to ensure case data is current and accurate and to streamline data entry.

The personal information collected and maintained by the USTP system will be accessed by the USTP government staff and cleared contractor staff. Additionally, the information may be shared with other law enforcement agencies as well as the private case trustees and other parties as appropriate. These routine uses are specifically covered under the USTP Systems of Records as published in the Federal Register on October 11, 2006 at 71 FR 59818.

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?

As required, debtor audit information will be shared with the US Attorney's Office, FBI, Civil Division or Criminal Division.

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?

The routine uses covering non-DOJ recipients are specifically covered under the USTP Systems of Records as published in the Federal Register on October 11, 2006 at 71 FR 59818. In general terms, the USTP may release information to:

Contractors, grantees, experts, consultants, and others performing or working on an assignment for the Program.

Bankruptcy Trustees to enable them to properly administer a case or to properly perform their duties.

Complainants or Victims to provide information as appropriate.

News Media as appropriate.

Members of Congress to provide information as appropriate.

Non-DOJ law enforcement or regulatory agencies as it relates to an investigation.

Courts or Administrative Body in response to a proceeding.

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.

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

Yes; however, subject to potential enforcement actions if failure is not satisfactorily explained. Much of the information in DAS is derived from the ACMS system, which automatically downloads the information about an individual's case contained in court records. Therefore, an individual does not have a right to decline to provide information that is delivered to DAS via ACMS. Regarding additional information that may be requested by auditors, an individual may decline to provide information, but may be subject to civil penalties for such refusal. These penalties include dismissal of the debtor's case, denial of discharge, or revocation of discharge.

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, debtors may not negotiate for particular uses of the information.

.

Section 8.0
Technical Access and Security

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

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

The data in DAS contains personally identifiable information; therefore, security is a key point. The possibility of users or administrators being able to access information inappropriately has been addressed by controlling access to the system and the ability to change data via user roles/privileges, as well as having forced system and audit logs copied off 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. There is always the possibility that authorized users can retrieve data and use it in irresponsible ways. However, training and reminding employees of their responsibilities, coupled with the ability to track system usage in the event wrongdoing should be discovered, helps mitigate this risk. All changes to data contained in DAS are logged in a journal. In addition, when transmitting data that contains social security numbers or other personal identifiable information, the Program has provided guidance to all staff on how to safe guard the transfer of limited official use data. At the present time, USTP system users have been given guidance on how to encrypt and password protect sensitive data using WinZip before transmission or saving to removable media.

Conclusion

Since it is the mission of the USTP to secure the just, speedy, and economical resolution of bankruptcy cases; 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; it is critical that the USTP continue to receive the relevant bankruptcy case and debtor audit information, including personal identifiers, in a timely and expeditious manner. Without this information, the USTP would be unable to fulfill its statutory requirements. The USTP reviewing officials feel that substantial measures are in place to protect the personal information collected and proper education has been and will continue to be provided to ensure this data is treated as “limited official use” by all Program staff, contractor staff, private trustees and associated law enforcement agencies.

Responsible Officials

If you have any questions regarding this document, please send your questions to:

Executive Office for U.S. Trustees
20 Massachusetts Avenue, NW
Suite 8000
Washington, DC 20530
Attn: Privacy Officer

or submit via Email to ustrustee.program@usdoj.gov

Approval Signature Page

_____ <<Sign Date>>

Jane Horvath
Chief Privacy and Civil Liberties Officer
Department of Justice