United States Trustees Program

Privacy Impact Assessment
for the
Automated Case Management System

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 Automated Case Management System (ACMS) was developed to support the United States Trustees Program (USTP) staff. ACMS serves as one of the main information systems supporting the USTP's mission to promote integrity and efficiency in the nation's bankruptcy system by enforcing bankruptcy laws, providing oversight of private trustees, and maintaining operational excellence. ACMS helps USTP staff efficiently review the case administration of bankruptcy cases. ACMS manages important case-related information, such as the debtor's estate detail and the history of the hearings, reports, pleadings, appointments, and fees for each case. Information in ACMS is downloaded from bankruptcy court electronic records or manually entered by authorized USTP system users.

ACMS is a legacy system that was developed in the mid-1980's. The system is comprised of 21 regional IBM RPG data files resident on a central IBM server accessible by USTP staff for analysis and reporting. ACMS provides the information necessary for the USTP to manage bankruptcy cases filed under chapters 7, 11, 12, 13 and 15 of Title 11 of the United States Bankruptcy Code. ACMS is being modernized to keep pace with the tracking of over 1 million new cases per year. ACMS helps the USTP to efficiently review the case administration of bankruptcy cases and assists with USTP civil enforcement efforts.

This Privacy Impact Assessment (PIA) replaces the PIA approved on August 24, 2006. That PIA described several different USTP information systems; this updated PIA only describes ACMS and other PIAs are being written for other USTP information systems.

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?

ACMS stores relevant case information including case numbers, debtor names, debtor social security numbers, company Employee Identification Numbers (EIN), debtor alias names, debtor addresses, and debtor attorney information. ACMS also maintains relevant case status information such as court orders, opinions, hearings, reports, pleadings, appointments, and fees along with associated dispositions.

1.2 From whom is the information collected?

The information in ACMS is originally collected from individuals who have filed for bankruptcy, and it appears in court filings in their bankruptcy cases. The bankruptcy case information contained in ACMS is primarily obtained directly from the United States bankruptcy courts either through a daily data file exported from the bankruptcy courts 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 bankruptcy courts to the USTP system via a secured (HTTPS) connection utilizing the existing Department of Justice Internet connection. Information can also manually be entered into ACMS by system users. Case status reports prepared by trustees also contain information that may be entered into ACMS.

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?

ACMS provides the information necessary for the USTP to manage bankruptcy cases filed under chapters 7, 11, 12, 13, and 15 of Title 11 of the United States Bankruptcy Code. The information described in Section 1.1 allows USTP staff to identify a particular debtor's case, review the status of a case, manage civil enforcement deadlines and monitor for possible fraud and abuse.

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:

[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 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 in ACMS, 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. These risks are minimized in part by the fact that the majority of the information collected in ACMS is obtained from the bankruptcy court filings. With the exception of the full social security number and some of the case status reports received from the case trustees, most of the information is available to the public via the court's Public Access to Courts Electronic Records (PACER) system. Despite this minimal risk, ACMS still contains safeguards against disclosure of this information. To mitigate the privacy risks, access to ACMS is limited by role-based access and such access is audited. In addition, the USTP has provided guidance to all staff on how to safeguard ACMS 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 ACMS.

Section 3.0
Uses of the System and the Information.

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

3.1 Describe all uses of the information.

ACMS provides the information necessary for the USTP to manage bankruptcy cases filed under chapters 7, 11, 12, 13 and 15 of Title 11 of the United States Bankruptcy Code. ACMS allows USTP staff to review the status of a case, manage civil enforcement deadlines and monitor for possible fraud and abuse. Many of the other USTP data collections systems will programmatically link back to ACMS on case number and will copy relevant case data and status information. Specifically, data is copied ("shared") from ACMS with the following USTP systems:

The Chapter 11 Quarterly Fee Information and Collection System (FICS). FICS is an accounts receivable system that assists the USTP with the noticing and collection of fees from chapter 11 debtors and tracks this activity throughout the life of the case. After receiving data from the bankruptcy courts, it is then sent to one of 95 USTP offices where the relevant data is manually keyed into ACMS. ACMS is then manually updated by USTP staff as the case progresses. Relevant ACMS case data and status information is transferred every 15 minutes to the FICS database. Once a month, FICS generates noticing (or delinquency as appropriate) information for each debtor and electronically transmits the data to a noticing contractor. The noticing contractor generates notices and mails them to the debtors (approximately 20,000 monthly). In addition, FICS provides USTP field offices online access to case status, financial transactions, disbursements, and event history information through the FICS Intranet Browser application. (No social security numbers are stored in FICS; however, company EINs may appear.)

Significant Accomplishments Reporting System (SARS). SARS allows USTP staff to record both informal and formal actions in the areas of civil enforcement, case administration and other significant activities. Basic case information, case number, debtor name and chapter are copied from ACMS to SARS as appropriate. (No social security numbers or additional personal information are stored in SARS.) The system also generates reports reflecting significant actions reported. The actions recorded in SARS closely correlate to the USTP civil enforcement efforts and provide part of the basis for the USTP annual report of significant accomplishments.

Criminal Enforcement Tracking System (CETS). CETS facilitates the accurate tracking of criminal enforcement efforts within the USTP, such as preliminary investigations by USTP staff, referrals to United States Attorney's offices and other law enforcement agencies, final dispositions and any assists with investigative efforts initiated by other DOJ components or outside law enforcement agencies. Basic bankruptcy case information, case number, debtor name and chapter, where applicable, are copied from ACMS to CETS as appropriate. The name(s) of persons who initially contacted the USTP (if a non-USTP employee), name of referring USTP employee, and name of contact person at recipient agency are also stored in CETS. (Social security numbers are only collected if relevant to identify a debtor.)

Means Test Review Management System - The Means Test Review Management System (MTR) was developed to support USTP review of the bankruptcy form that assesses debtors' current monthly income required under the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA). As of October 17, 2005, certain debtors are required to file current monthly income forms along with their petitions 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 current monthly income and Means Test calculation forms data to verify the results. In addition, the MTR System tracks 11 U.S.C. § 341 creditors' meeting dates and associated due dates for required United States Trustee Presumption of Abuse Statements and related motions. Basic case information, case number, debtor name, address, chapter, debtor attorney name, and judge name are copied from ACMS to MTR as appropriate. (No social security numbers or additional personal information is stored in MTR.)

The information collected and maintained by the ACMS system will be accessed by the USTP government staff and cleared contractor staff. Information that is received directly from the AOUSC via 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.)

No, the system does not have data mining functions. Users can query ACMS to generate data and reports that will show the status of a case, indicate upcoming deadlines, and identify potential patterns that may be indicators of fraud and abuse. Subsequent analysis by investigators can be used to determine the veracity and usefulness of any such correlations.

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

The USTP established internal minimum ACMS standards in 1992 and updated them in 2006. These standards were designed to improve the efficiency and accuracy of the collection of bankruptcy case management data by ensuring that the required data elements are being entered and used in a uniform standard by all regions. In addition, the USTP has established a Data Integrity Group (DIG) to ensure the appropriate data entry and review protocols exist for the data

collections comprising the USTP system. The DIG also conducts periodic reviews in addition to the periodic certifications required by the USTP field management. ACMS data is primarily obtained directly from the bankruptcy courts either through a daily data file or manually entered from documents filed with the courts. ACMS data is reviewed and compared against data in the court systems, as appropriate. Various quality control reports are run routinely to ensure all requisite case data has been received from the courts and entered into ACMS. Additional data quality checks are performed using the AOUSC's official data to review for any anomalies with regard to filing statistics. This review is performed prior to the publication of the USTP Annual Report of Significant Accomplishments.

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 ACMS 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. Audits are done at regular intervals to ensure that there is no improper use by users. In addition, guidance is provided on how to safeguard Limited Official Use data.

Security for ACMS data is provided by the IBM operating system and by controls in the ACMS application. User accounts on the IBM system are setup as part of a "group" account. There is a separate group account for each region. The group account gives the user read-only access to the data in the user's region and to use program libraries specific to the user's region. This prevents users from accessing data outside of their own region. The ACMS application is menu-driven and includes a menu control file that limits the menus to which the user has access. Menu access is assigned at the regional level and is based on the individual user's job function within that region.

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 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 United States 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?

All the information described in Section 1.1 may be shared as appropriate in connection with a bankruptcy fraud investigation or appeal. The purpose of the sharing would be for official law enforcement purposes, such as referring a case to the United States Attorney's Office for further investigation.

4.3 How is the information transmitted or disclosed?

Information from ACMS is transmitted to internal DOJ recipients (outside of USTP) via email, facsimile or hard copy.

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 information internally is an increased risk of unauthorized use or disclosure of ACMS data. As stated in 2.3, this risk is minimized because the majority of the information collected in ACMS is obtained from bankruptcy court filings. For the most part, the collected information is publicly available via the court's PACER system, except for the full social security number, some case status reports received from the case trustees (and not also filed with the courts), attorney notes and possibly other anomalies. To reduce the risk of disclosure when transmitting data that contains social security numbers or

other PII, 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 Department components direct access to the information and only sharing information when there is a legitimate need to know for official purposes.

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 USTP routinely shares data with the bankruptcy trustees to enable them to properly administer a case or perform their duties. Information that is received directly from the AOUSC via 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?

The information described in Section 1.1 from ACMS may be shared with the bankruptcy trustees or those with a legitimate need-to-know relating to the successful administration of a case or the possible identification of fraud or other illegal activity, such as a serial filer abusing the system, a creditor charging excessive fees, inappropriate practice of law or possible hidden assets not disclosed.

5.3 How is the information transmitted or disclosed?

Information is transmitted to external recipients on a case-by-case basis, in either hard copy (paper) or using email. When transmitting data that contains social security numbers or other PII, the USTP has provided guidance to all staff on how to safeguard 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 (which will provide 256 AES encryption) before transmission.

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.) which leaves DOJ facilities requires additional protection and must be encrypted with USTP-approved encryption software.

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

Any data that is part of an investigative file is treated as Limited Official Use data. Contractors are required to sign non-disclosure and confidentiality agreements for access to USTP data. Bankruptcy trustees are provided guidance for safeguarding Limited Official Use data, which includes PII.

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 ACMS specific training is given to external entities before transmitting information from ACMS to them. However, USTP does conduct a training course for the bankruptcy trustees on general case administration matters.

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

While the ACMS data is not audited, USTP does routinely audit the bankruptcy trustees' operations 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 potential privacy risk with sharing information externally is an increased risk of unauthorized use or disclosure of ACMS data. To mitigate this risk, external users are notified if the data being provided contains Limited Office Use data. To reduce the risk of disclosure when transmitting data, USTP staff has been provided guidance on how to safeguard the transfer of Limited Official Use data. In addition, contractors must use the government systems where appropriate to transmit data in a closed environment or to protect files when transmitting electronically. As stated in Section 2.3, the risk is also minimized because most of the bankruptcy case information collected in ACMS is available to the public via the court's PACER system. Other entities are not given direct access to the ACMS system, and information is only

shared when there is a legitimate need to know and such sharing is authorized under the Privacy Act. Bankruptcy trustees' operations are audited routinely to ensure they are compliant with USTP policy and have appropriately secured systems.

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

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 in ACMS under the Privacy Act, 5 U.S.C § 552a. However, the information maintained in ACMS is primarily obtained directly from the bankruptcy courts and changes in ACMS would not change court records. Individuals can amend their records in the bankruptcy courts' system, which in most instances would then be updated in ACMS.

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 Departmental 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 7.1. Additionally, if an individual exhausts his 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 the system.

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?

All USTP staff may be granted access to ACMS. Depending upon their role, they will be granted read only or read/write access. Contractors providing development and general user support have access to the system.

When users are created in ACMS, their security profiles are edited to give them the access they require. After users complete the security sign-on, they have access to data for one location or "group designator" within the full regional database. In addition, a user's security profile can also limit which menu options in ACMS the user will have access to. This limits access to sensitive menu options, including the Security Menu itself. Access is closely monitored for certain menu options.

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 for ACMS.

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

Yes, user "roles" are controlled by a user's Security Profile. The user Security Profiles are edited to give users the access they require. In addition, a user's Security Profile can also limit which menu options in ACMS the user will have access to. This limits access to sensitive menu options, including the Security Menu itself. Access is closely monitored for certain menu options.

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 ACMS 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 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. These events are reviewed weekly by the Security Team. A database administrator regularly runs a report of locked accounts and provides the report to the System Owner and to the Security Team for review. All logins and access are tracked within the database. From a management control perspective, annual security training and the Rules of Behavior Certifications that have to be signed, 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. At the current time, access to ACMS is not dependent upon completion of the annual security training; however, the USTP Information Systems Security Manager does ensure that all users complete their annual training.

A memorandum, dated October 11, 2006, from the Acting Deputy Director was sent to all employees (1) reminding employees of their responsibility to safeguard and protect personally

identifiable information from inadvertent access or disclosure, and (2) establishing new reporting requirements for incidents involving data loss and personally identifiable information. This memorandum has been posted on the USTP Intranet site.

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 on May 9, 2008.

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

The data in ACMS contains personal information. Therefore, ensuring adequate security is critical. 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. There is always the possibility that authorized users can retrieve their own data and use it in irresponsible ways. However, training and reminders to employees of their responsibilities, coupled with the ability to track system usage if wrongdoing should be discovered, helps mitigate this risk. All changes to data contained in ACMS are logged in a journal. The information that is captured includes the username, date, time, workstation address, and the data changed.

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 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 to identify solutions that best incorporate the latest information system security controls required by FISMA. With each new iteration of the System, the current technologies are evaluated for functional and security benefits.

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

The USTP IT Staff has a well-developed Configuration Management and Data Management process in support of the System Development Life Cycle. Every stage 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.

9.3 What design choices were made to enhance privacy?

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. Security "groups" that provide access to data and program libraries in a specific region were designed to safeguard Limited Official Use data. 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. Without this information, the USTP would be unable to fulfill its statutory requirements. The USTP reviewing officials conclude 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 USTP staff, contractor staff, and private trustees.