United States Trustee Program

Privacy Impact Assessment
for the
Credit Counseling/Debtor Education System (CC/DE 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:	May 23, 2011

(February 2011 DOJ PIA Form)

Introduction

The Credit Counseling/Debtor Education (CC/DE) System was developed to support the United States Trustee Program's (USTP) approval process for reviewing applications submitted for consideration as approved credit counseling agencies (agency) or approved providers of a personal financial management instructional course (provider), referred to as debtor education, under the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA). The CC/DE System facilitates the tracking of the receipt of the application, the review process and final determination, as well as notification to the courts and general public of the approved agencies and providers via the USTP's website where the list of approved agencies and providers is published. For the approved agencies and providers, the CC/DE System allows for the tracking of the associated renewal process and any complaints received regarding any of the agencies or providers. Basic applicant information is captured in the system, such as applicant name, title, company name, address, email address, phone number, fax number, social security number (when the debtor education provider is an individual), or employer identification number (EIN), plus names and address of all owners, officers, directors, partners, or trustees. The CC/DE System also captures the name, title, company name, address, email address, and phone number of complainants, along with any names of individuals perceived to be harmed by an agency or provider's actions other than the complainant.

In addition, as part of the CC/DE System, there is a web-based database that enables the agencies and providers to issue certificates of completion to their clients. Agency and provider information is captured in the system, such as counselor name and company name, as well as the individual's name in the case of debtor education certificates, to track more easily when duplicate certificates are issued. The case number is also captured when issuing debtor education certificates only. No social security numbers of the individual clients or debtors are stored in the CC/DE System. The web-based system utilizes separate DOJ servers located in a secure DOJ facility.

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?

Credit counseling agencies submit a credit counseling application while debtor education providers submit a debtor education application. Along with the status of the application the CC/DE System stores the basic applicant information in the system, such as, applicant name, title, company name, address, email address, phone number, fax number, EIN or social security number (when the debtor education provider is an individual), plus names and address of all owners, officers, directors, partners, or trustees. The CCDE System also captures the name, title, company name, address, email address, and phone number of complainants, the particulars of the complaint, and its resolution. The complaint record may include names of individuals perceived to be harmed by an agency or provider's actions other than the complainant.

The web-based certificate issuance system for credit counseling certificates captures the date and time counseling was provided, the bankruptcy court and division in which the certificate would be filed, the method of service delivery (i.e. via telephone, internet, or in-person), the counselor's name and whether a debt management plan was prepared. For credit counseling certificates, the client's name is entered and appears on the certificate, but is not stored in the CC/DE System. For debtor education certificates, the above information is collected. In addition, the individual debtor's name and bankruptcy case number is entered, stored in the system, and appears on the certificate. No other personal information regarding any individual receiving credit counseling or debtor education is captured in the CC/DE System. No social security numbers of clients or debtors are stored in the CC/DE System.

1.2 From whom is the information collected?

The information is collected from the agencies and providers who have applied to offer approved credit counseling and/or debtor education services under the BAPCPA. Limited information is also collected from those individuals who have filed for bankruptcy and are receiving their certificate of debtor education. Complainants provide information about issues they may have had with the performance of specific agencies or providers.

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 BAPCPA requires individuals filing for bankruptcy to complete a credit counseling course (prior to filing) from an USTP approved credit counseling agency and to then take a debtor education course from an USTP approved debtor education provider, prior to obtaining a discharge in bankruptcy. The BAPCPA also requires the USTP to thoroughly review each credit counseling agency and debtor education provider's qualifications and to approve only those applicants that meet the statutory requirements for approval. The data collected from applicants is used to determine whether they meet the statutory and regulatory requirements to receive approved status from the USTP. The CC/DE System was developed to support the USTP's approval process for reviewing applications submitted for consideration. Without this data, the USTP cannot perform its statutorily mandated duty to approve only qualified agencies and providers. As a result, debtors would be unable to fulfill their statutory duty to complete credit counseling or debtor education from USTP approved agencies and providers.

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).

In addition, BAPCPA requires those individuals filing for bankruptcy to complete a credit counseling course prior to filing and to then take a debtor education course prior to obtaining a discharge in bankruptcy. Under BAPCPA, the USTP is tasked with approving agencies and providers of these services. See 11 U.S.C. § 111. The USTP also promulgated a regulation to govern the application process. The regulation, which is entitled "Application Procedures and Criteria for Approval of Nonprofit Budget and Credit Counseling Agencies and Approval of Providers of a Personal Financial Management Course by United States Trustees," 71 Fed. Reg. 38,076 (July 5, 2006) (codified at 28 C.F.R. § 58.15 – 58.17, 58.25 – 58.27), sets forth the procedures for the review and approval of applicants seeking to provide credit counseling or debtor education services.

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 collecting only the minimum amount of personally identifiable information (PII) that is necessary for USTP staff to perform a review of applicants' qualifications. To mitigate the privacy risks, access to the CC/DE System 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 this 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 the CC/DE System. Furthermore the risk of inaccurate data is minimized because the majority of information collected in the CC/DE system is provided directly by the applicants seeking to become approved agencies or providers. In the case of complaints received, the information collected is provided directly and voluntarily by the complainants.

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 CC/DE System provides the information necessary for the USTP to review, approve and renew the applications submitted for providing credit counseling and debtor education services under BAPCPA, as well as tracking any complaints received about the approved agencies or providers and providing a national system for issuing certificates of completion. The information in the CC/DE System will be accessed by the USTP CC/DE staff to track the status of the application review, acceptance and renewal process, receipt and follow up process regarding complaints, and all certificates issued. Management reports will be generated for the USTP CC/DE staff to provide overall status and details as well as reports to assist the USTP field staff with verifying the accuracy of certificates filed with the courts and to ensure BAPCPA requirements are met.

The PII collected and maintained by the CC/DE system will be accessed by the USTP government staff and approved contractor staff. 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 System of Records Notice (SORN) as published in the Federal Register. See 71 Fed. Reg. 59,818 – 59,830 (Oct. 11, 2006).

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 CC/DE system does not perform data mining.

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

The EOUST staff managing the review and approval process undertakes ongoing quality reviews. EOUST staff review and confirm the accuracy of the personnel, judicial district, location, and contact information data in the database prior to a final approval of an agency or provider. Additional quality reviews take place on a periodic basis. Every two weeks, the database is updated, and EOUST staff conduct spot checks to confirm that known changes to agency and provider information during the two week period are reflected in the database. On a quarterly basis, lists of inactive agencies and providers are updated from the database, and EOUST staff review the database to ensure that withdrawals, denials, and other cessations of approval are reflected correctly on both the list and the database.

In addition, the field office staff and private trustees review certificates filed with the courts. Any anomalies identified are forwarded to the local office of the U.S. Trustee and the Executive Office in Washington, DC as required for further reviews. Quality review reports are generated to identify discrepancies or false certificates.

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 the CC/DE System has been reviewed and approved by the National Archives and Records Administration (NARA). The retention period for data in the CC/DE 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 CC/DE System is limited to certain authorized users in the Executive Office located in Washington, D.C. Authorized users must enter individual user ids and passwords. Based on the user's role in the 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 in how to safeguard Limited Official Use data.

Access to the certificate issuance website of the CC/DE System is limited to approved agencies and providers. Users must enter individual user ids and passwords and can only view data that pertains to their particular agency or provider.

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 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 the CC/DE System 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 data in the CC/DE System. To reduce the risk of disclosure when transmitting data that contains 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?

Information from the CC/DE System is not generally shared with non-DOJ recipients, other than the applicants (credit counseling agencies and providers) themselves. When information is shared with non-DOJ recipients, the sharing of information is accomplished through the routine uses specified under the USTP's SORN.

5.2 What information is shared and for what purpose?

Information is generally shared with the applicants in order to facilitate the review of their applications. When information is disclosed to non-DOJ recipients, it is done so in accordance with the purposes identified in the USTP's routine uses in its SORN.

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 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.

The approved agencies and providers may access the certificate generation website to create certificates and may print the certificates or save them as PDF files for transfer to their customers.

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.

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

The only external users (non-USTP) that receive access to the CC/DE system are approved credit counseling agencies and providers. Their access is limited to printing or saving certificates of completion. They receive access to detailed on-line written instructions on how to perform this limited function when they are approved by the USTP. Additionally, approved credit counseling agencies and providers are audited routinely to ensure they are compliant with USTP policy.

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

The USTP routinely audits approved agencies and providers to ensure they are compliant with USTP policy.

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 data in the CC/DE System. To mitigate this risk, external users are notified if the data being provided contains Limited Official 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. Only approved agencies and providers are given access to the CC/DE System as external users, and they may only print or save certificates of completion. These agencies and providers receive access to detailed on-line written instructions on how to perform this limited function when they are approved by the USTP, and the USTP routinely audits them to ensure they comply with USTP policy.

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?

The USTP published a SORN in the Federal Register that covers the collection of information contained in the CC/DE System and the application process is posted on the USTP website at: http://www.usdoj.gov/ust/eo/bapcpa/ccde/index.htm. In addition, the instructions to the debtor education application contain a Privacy Act Statement that states, "Section 111 of title 11, United States Code, authorizes the collection of this information. The primary use of this information is by the Executive Office for United States Trustees to approve providers of instructional courses concerning personal financial management. Additional disclosure of the information may be to district and regional offices of each United States Trustee. The information will not be shared with any other agencies unless allowed by law. Public Law 104-134 (April 26, 1996) requires that any person doing business with the federal government furnish a Social Security Number or Tax Identification Number. This is an amendment to title 31, Section 7701. Furnishing the Social Security Number, as well as other data, is voluntary, but failure to do so may delay or prevent action on the application."

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

Yes, submission of an application is entirely voluntary.

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?

Submission of an application is voluntary. However, if applicants wish to be considered for approval as an approved agency or provider, applicants are informed of the uses of the information in the CC/DE System and are required to consent to these uses by signing the application.

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 SORN that covers the collection of information has been published in the Federal Register, and because an applicant must voluntarily submit an application, the risk that an individual would provide information without informed consent is mitigated. The SORN

provides the individual with transparency concerning the USTP's collection, use, and maintenance of the information in the CC/DE System.

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. However, any information that is involved in a law enforcement referral, and is transferred to records maintained under the USTP's system of records UST-004, U.S. Trustee Program Case Referral System, 71 Fed. Reg. at 59,825, is exempted from the access and amendment provisions pursuant to 5 U.S.C. § 552a (j)(2). See 28 C.F.R. § 16.77.

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 the USTP's SORN 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 Section 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?

Access to the CC/DE System is limited to the Executive Office located in Washington, D.C. In addition, approved agencies and providers will have access to the certificate issuance website in order to print or save certificates.

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 the CC/DE System.

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

Yes, based on the user's role in the review process, a comparable role is granted to the end user at the application and database level. For example, some users are given read–only access, some users have the ability to add comments, and an even smaller number of users can enter/edit data with only a few having delete capabilities.

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. This 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 for obtaining an account are established as defined in Section 3.5. The procedures for creating and maintaining system access are audited regularly and are part of the annual 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?

Roles and permissions are designed 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 and reviewed to ensure they reflect current permissions. 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 DOJ Computer Security Awareness 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 March 2009; this is the most recent certification and accreditation.

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

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. 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 system changes to the data are logged in a journal.

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 General Accounting Office and Office of Management and Budget's Raines Rules, the CC/DE 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 compete 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.

During development, a security review as well as configuration and data management validation were completed. Data integrity, security and privacy concerns are reviewed as part of the System Development Life Cycle process. These requirements are part of the system design documentation and cannot be promoted during development if these steps are not addressed.

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. 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

The BAPCPA requires individuals filing for bankruptcy to complete a credit counseling course prior to filing bankruptcy and to then take a debtor education course prior to obtaining a discharge in bankruptcy. These services must be provided by agencies and providers approved by the USTP. Thus, it is critical that the USTP be able to thoroughly review applications to ensure applicants are qualified to perform these services. Without the information collected in the CC/DE System, the USTP would be unable to fulfill its statutory requirements.