Justice Management Division

Privacy Impact Assessment
for the
Consolidated Debt Collection System

Issued by:
Barbara Bush, JMD Acting General Counsel

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: February 8, 2012

(February 2011 DOJ PIA Form)

Introduction

The Department of Justice (DOJ) is responsible for the enforced collection of settlements and court-ordered monetary judgments on behalf of the United States, as well as on behalf of other aggrieved parties, such as state, local, or tribal governments. The DOJ sues debtors who have reneged on their responsibilities to pay their debt. Such debts may arise from the myriad of federal programs under which federal agencies loan money directly to our citizens; guarantee or ensure loans that citizens make from private financial institutions; that arise from amounts due federal agencies from fees, leases, services, civil penalties, overpayments, or other similar sources. In addition, DOJ must enforce the monetary judgments awarded by the courts as the result of criminal litigation.

Prior to the implementation of the Consolidated Debt Collection System (CDCS) the DOJ used multiple applications/tools to track and manage debt collection activities and financial litigation efforts conducted by various entities within the Department. These entities included the 94 U.S. Attorney's Offices, associated contracted private counsel, and six DOJ litigating divisions (Anti-Trust Division, Civil Division, Civil Rights Division, Criminal Division, Environment and Natural Resources Division, and Tax Division).

The Consolidated Debt Collection System (CDCS) merged these multiple systems into a single, standard application that improves data integrity, provides for a central system across the DOJ, facilitates better communication on debt collection matters among the DOJ components, supports the implementation of department-wide debt collection initiatives, provides for better accountability and timely reporting, and centralizes administrative functions such as the generation of routine correspondence (statements, default letters, etc.) and payment processing. Access to CDCS is limited to authorized Department of Justice employees and DOJ contracted staff. DOJ personnel access CDCS through the Justice Consolidated Network (JCON). Secure Remote access is provided to DOJ staff through a virtual connection.

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

1.1 What information is to be collected?

Determined[1] and undetermined[2] financial matters are referred to the DOJ for litigation, and ultimate collection or resolution of the debt. CDCS cannot currently accept

[1] Determined claims are evidenced by a signed document, agreement, promissory note, etc.
[2] Undetermined claims require some litigation action, acknowledgement, agreement, or settlement to establish the amount of the debt.

electronic referral documents. Claim referral information is received in hard-copy and entered in the CDCS database. Hard-copy claim data may include: (a) personal data (e.g., name, date of birth, taxpayer identification number, address information, employment information, and credit data); (b) claim details (e.g., value and type of claim (benefit overpayment, loan default, bankruptcy, etc), documents evidencing the claim); (c) demand information, settlement negotiations, and compromise offered; (d) account information (e.g., debtors' payments, including principal, penalties, interest, and balances, etc.); and (e) information regarding debtors' employment, assets, ability to pay, property liens, etc.

Additionally, throughout the life of the claim, data may be entered into the system by CDCS users or added to the system through automated interfaces. Such data may include; (a) additional/updated debtor contact information; (b) dates regarding the litigation of the case (e.g. court filings, pleadings, judgment award or discharge information, court orders, and settlement agreements); (c) information on the status and disposition of the case; (d) names and contact information of individuals associated with the debt (e.g. attorneys, whistleblowers, etc.); and (e) payment data (e.g. banking information, data related to the Treasury Offset Program (TOP), offsets of the salaries and benefits of federal employees or members of the Armed Forces, and other administrative offsets). The system may contain additional information related to the negotiation, compromise, or settlement of debts owed to the United States and others, or related to the administrative management of debt collection efforts.

1.2 From whom is the information collected?

Most information is provided to the Department of Justice during the referral process by creditor or investigative agencies (federal, state, or local governments). Additional information is obtained during the litigation and collection processes, directly from the debtor (e.g. debtor interviews) or indirectly via standard collection practices (e.g. skip tracing, credit reports, record searches, etc.). Other information may be obtained from federal, state, local, tribal, territorial, foreign governments or municipalities; private organizations or other individuals (e.g. attorney representatives) who may have information regarding the debt, the debtor's ability to pay, or information relevant or necessary to assist in the resolution of the debt.

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

2.1 Why is the information being collected?

CDCS collects personal information in order to locate and correspond with debtors, as well as to identify and evaluate debtor assets for the ultimate resolution of the debt. Personal information is necessary to properly track and collect fines and other debts owed to the Department of Justice, other Government agencies, and third parties. The information is used to perform legal, financial and administrative services associated with the collection of debts due the United States, including related negotiations, settlements, litigation, and enforcement efforts.

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

The collection of this information is authorized by the Debt Collection Act of 1982, Pub. L. No. 97-365, 96 Stat. 1749 (1982), as amended by the Debt Collection Improvement Act of 1996, 31 U.S.C. §§ 3701-3720E (original version at Pub. L. No. 104-134, 110 Stat. 132 (1996)), and the Federal Debt Collection Procedures Act of 1990, 28 U.S.C. §§ 3001-3307 (original version at Pub. L. No. 101-647, 104 Stat. 4789 (1990)) and Chapter 31 of Title 44, United States Code.

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.

During the acquisition process, specific security risks were identified. As a consequence, security clauses, constraints, controls and requirements were incorporated into the Statement of Work for the CDCS contract. Additionally, during the development and implementation process, security risks specific to privacy were further discussed along with mitigation strategies for those potential risks.

Potential privacy risks identified and mitigation strategies include:

Potential Risk	Mitigation Strategies Employed
Possible breach of agency databases	User access controls of electronic data and encryption of data both at rest and while being transmitted across the database are employed. User access controls include requiring passwords to be changed every 90 days, disabling access after 90 days of inactivity, using two-factor-authentication for remote access, and auditing system functions.
Loss or theft of computer equipment containing privacy data	Security access controls, including encryption of portable mobile devices, are employed on devices containing CDCS data. Other standard physical security practices such as controlled access to facilities, cameras, visitor logs, credentials, and employee training are also used. Staff members are reminded periodically via memoranda and emails of their responsibility to secure privacy data.
Loss or theft of paper documents or electronic media containing privacy data.	Hard-copy material containing privacy information is shredded or burned bi-weekly. Containers for this material are locked with only the Security Program Manager and Facility manager maintaining a key when the receptacle is in a common location. When the container is in an individual office, only the person assigned to the office and the Security Manager have keys. Staff members are reminded periodically via memoranda, emails and through annual awareness training of their responsibility to secure privacy data.

Unauthorized disclosure of Privacy data	A notice of penalties (including Privacy Act and IRS civil and criminal penalties) for unauthorized disclosure is included in the Rules of Behavior, and is part of the annual IT Security Awareness and Training for all staff.

In addition, deterrent controls, implemented to address all risks identified include:

- Warning Banners and Confidentiality Agreements;
- Background checks and security clearances conducted for all personnel with access to CDCS commiserate with the level of risk identified by the DOJ, Personnel Security Group;
- Exit procedures for departing employees and contractors that include the prompt disabling of accounts and access rights to all data.

Section 3.0 – Uses of the System and the Information.

3.1 Describe all uses of the information.

The data contained in CDCS is used by the Department of Justice and its agents to perform the following activities and related debt-collection efforts:

(a) To correspond with debtors through the generation and mailing of documents, email correspondence, or phone calls;

(b) To locate and track debtors and debtor assets, performing skip trace activities as necessary to resolve returned mail or wrong numbers;

(c) To conduct litigation to collect debts due the United States;

(d) To effectively enforce the collection of debts through both pre-judgment and post-judgment remedies, such as garnishment, liens and Treasury Offset;

(e) To identify debtors owing more than one debt and when appropriate coordinate collections; and

(f) To perform financial and administrative tasks associated with the collection of debts, posting to debtor accounts, and distribution of funds.

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. Data on this system is not used for data mining.

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

System auditing, data integrity reports, and quality control procedures and reports are employed by authorized users of the system to cross-check data in the system for accuracy. Data obtained from other Federal agencies may be used to validate information already in CDCS.

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)?

Master File records for this information system are retained for seven years after close of the case, in accordance with the National Archives and Records Administration (NARA) Schedule (N1-060-08-02). Case information is maintained by Department of Justice litigating components in accordance with their NARA approved retention schedules for litigation records.

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

In accordance with the NIST SP 800-53 security controls, AC-02 (*ACCOUNT MANAGEMENT*[3]) and AU-06 (*AUDIT REVIEW, ANALYSIS, AND REPORTING*[4]), CDCS establishes, monitors, and maintains all user accounts in accordance with DOJ standards. Log-on attempts (successful and unsuccessful) are captured routinely as part of the audit log. Guest, anonymous, and temporary user accounts are not allowed on the system. When staff is terminated, transferred, or their need to access the information system changes, access is removed or amended promptly. User access is

[3] **AC-02 Account Management security control**: The organization manages [accounts], including: identifying authorized users of the information system and specifying access privileges; establishing, activating, modifying, disabling, and removing accounts; notifying account managers when information system users are terminated, transferred, or information system usage or need-to know/need-to-share changes; deactivating; granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization.

[4] **AU-06 Audit Review, Analysis, and Reporting**: Review and analyze information system audit records for indications of inappropriate or unusual activity, and report findings to designated organizational officials.

reviewed periodically by the system security officer. System data is maintained in accordance with DOJ Order 2640.2F, "Information Technology Security" and related authorities, including OMB guidance on safeguarding personally identifiable information. Also, FISMA-mandated continuous monitoring requirements (NIST SP 800-53) provide assurances that privacy-applicable controls are assessed on an ongoing basis consistent with what was approved by the Department Authorizing Official when the system was given approval to operate (ATO). Further, CDCS enforces the automatic locking (disabling) of user accounts after three invalid logon attempts.

The DOJ warning banner, displayed when users first access CDCS, notifies users that they are subject to monitoring while using the CDCS system, and may be subject to criminal prosecution and civil or criminal penalties for any unauthorized use. It reads:

This computer system is property of the United States Department of Justice. The Department may monitor any system activity and retrieve any information stored within this system for law enforcement, adherence to acceptable use policy, or other purposes. By using this computer system, you are consenting to such monitoring and information retrieval. Users should have no expectation of privacy regarding information stored, processed, or communicated with this computer system, including removable media.

Unauthorized use, or attempted unauthorized use, of this computer system may subject the user to criminal prosecution and criminal or civil penalties.

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

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

CDCS data is shared with the DOJ components and offices nationwide that have debt collection and enforcement records and/or responsibilities. These include the 94 U.S. Attorneys' Offices; associated contracted private counsel; the Executive Office for U.S. Attorneys; JMD Offices of Debt Collection Management (DCM) and the Chief Information Officer (OCIO); JMD contracted staff, and six DOJ litigating divisions (Antitrust Division, Civil Division, Civil Rights Division, Criminal Division, Environment and Natural Resources Division, and Tax Division).

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

Information is shared with each recipient component or office for the purpose of performing legal, financial, and administrative services associated with the litigation and

collection of debts due the United States. The information provided to each component or office is limited by the assigned system access privileges.

Access is limited to only those cases that an individual has some responsibility to litigate, collect, enforce or administer (post payments, enter claim information, etc.) An individual's access to CDCS is constrained first by the Component where the user works, and then limited by subcomponent, and district or office. Access is even further restricted by the specific user role. For example, a lead technician will have access to all the data in that office; while technicians can only access those cases they are assigned. An attorney in the same office may be able to view all of the debts within an office, but may not be able to update them.

Within CDCS, access is managed through system security tools and the logical separation of data according to the minimum amount of access necessary to perform assigned duties. Users are only allowed access to data to the extent they have a demonstrated and legitimate need to view or update that data, in support of departmentally authorized debt collection activities.

On occasion, the litigation of a case or the enforcement of a collection action may be shared between components, or offices within a component. For example, the Civil Division may choose to request that the U.S. Attorney Office in the district where the debtor resides enforce or assist with the collection action after a judgment has been awarded. In those cases, the responsibility for the case will change to the office that has been assigned the collection, and the component requesting the 'assist' will retain the ability to view, but not update the case.

4.3 How is the information transmitted or disclosed?

Sharing a claim between components, as described in section 4.2, is performed electronically via CDCS. The requesting component sends a workflow request to the receiving office via CDCS. The receiving office accepts the request. Once it has been accepted, the case becomes accessible to the receiving office. The new responsible office then sends a workflow notice to the requesting component that allows them to view the claim. Data does not leave the database electronically or in hard copy. Sharing in CDCS represents only a transfer of ownership rights within the database.

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

(a) Potential privacy risks may include:

Potential Risks	Mitigation Strategy
Possible breach of agency/contractor databases	Mitigation of risk is provided through user access controls of electronic data and encryption of data at rest and data being transmitted across the database. User access controls include requiring passwords to be changed every 90 days, disabling access after 90 days of inactivity, using two-factor-authentication for remote access, and auditing system functions.
Unauthorized disclosure through misdirected requests	Only a minimum of information is sent in the initial workflow request. The workflow does not include sensitive privacy data (i.e. – Taxpayer Identification Numbers) or details of the debt. The request includes CDCS account# and debtor name.

In addition, deterrent controls in the form of Warning Banners, Rules of Behavior, Confidentiality Agreements and auditing are in place. Background checks and/or security clearances, coupled with access restrictions, are required for personnel prior to being granted access to system data. Finally, exit procedures for departing employees and contractors include the prompt disabling of accounts and access rights to all data.

Section 5.0 – External Sharing and Disclosure

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

Data gathered during the course of the litigation and collection process may be shared with referring or “client” agencies from whom the debts originated (e.g., Department of Education, Department of Veterans Affairs, Department of Treasury, Health and Human Services, etc.,) and other entities set forth in the routine uses of the Privacy Act System of Records, JUSTICE/DOJ-016.

In addition, information may be shared with the Department of Treasury, for the potential offset of benefits, as part of the Treasury Offset Program (TOP) in accordance with 26 U.S.C. § 6402(d); shared with the Credit Alert Interactive Verification Reporting System (CAIVRS) administered by the Department of Housing and Urban Development for the purpose of evaluating the credit worthiness of Federal loan applicants, and shared with other agencies in accordance with data matching programs related to debt

collection efforts.

5.2 What information is shared and for what purpose?

Periodically, referring agencies may be provided with status information on the cases they have referred to the Department of Justice. Data shared with a referring agency may include updated debtor contact information; dates regarding the litigation of the case (e.g. court filings pleadings, judgment award or discharge information, court orders, and settlement agreements); information on the status and disposition of the case; names and contact information of individuals associated with the debt (e.g. attorneys, whistleblowers, etc.); and payment data (e.g. banking information; data related to the Treasury Offset Program (TOP), offsets of the salaries and benefits of federal employees or members of the Armed Forces, and other administrative offsets); or information related to the negotiation, compromise, or settlement of debts owed to the United States and others, or related to the administrative management of debt collection efforts. This data is generally provided in the form of a scanned report or excel file.

Once a judgment has been obtained, and a claim is evidenced in public record, information may be shared with the Department of Treasury, for the potential offset of benefits, as part of the Treasury Offset Program (TOP) in accordance with 26 U.S.C. § 6402(d); shared with the Credit Alert Interactive Verification Reporting System (CAIVRS) administered by the Department of Housing and Urban Development for the purpose of evaluating the credit worthiness of Federal loan applicants, and shared with other agencies in accordance with data matching programs related to debt collection efforts.

Data may also be shared pursuant to Court order or in connection with legitimate law enforcement activity or for other purposes as set forth in the Privacy Act System of Records, JUSTICE/DOJ-016.

5.3 How is the information transmitted or disclosed?

External entities do not have direct access to CDCS data. The transfer of information is initiated by DOJ. All data is encrypted during transfer. Information is transferred via a secure (encrypted) government website via Virtual Private Network (VPN).

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

The security and privacy of data shared is documented in mutual Data Matching Agreements and Memoranda of Understanding (MOU) documents.

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

There are no outside agency users of CDCS. Only DOJ employees and DOJ contracted staff have direct access to CDCS. Therefore no CDCS training is required or provided to users from agencies outside of DOJ

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

No provisions are currently in place for auditing recipients' use of information. Should DOJ become aware of misuse of the data, appropriate steps would be taken, including suspension of data sharing activities.

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

Data is shared with external agencies in accordance with established public law, and federal mandates. External entities do not have direct access to CDCS data. Data provided to client agencies includes the status of debts referred to the DOJ for collection.

In addition during the course of collecting debt, data may be shared with external entities to assist with the collection effort. These disclosures are limited to only what is needed to identify the debtor, assist with the collection effort by performing an offset or prevent the debtor from receiving additional Federal benefits before the delinquency is resolved. Data is shared securely, in accordance with agreed upon terms identified in Computer Matching Agreements, Memoranda of Understanding, or Inter-Agency Agreements as signed by appropriate Agency Officials. These agreements outline the appropriate uses of the data and security requirements that must be met for data sharing.

Section 6.0 – Notice

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?

DOJ provides constructive notice to record subjects through publication in the Federal Register of systems notices, Privacy Act System of Records Notice JUSTICE/ DOJ-016, "Debt Collection Enforcement System," which apprises the public that this information may be collected and used for authorized purposes. Additionally, a specific 60 day notice is provided prior to an individual being referred to the Treasury Offset Program.

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

No. The collection of this information is required and authorized for debt-collection and related law enforcement activities.

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. The collection of this information is required and authorized for debt collection and related law enforcement activities.

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

The privacy risk identified would be the failure of persons to be aware that their information may be collected and what it will be used for. To mitigate this risk, DOJ publishes a Privacy Act System of Records Notice (SORN) for the compilation of debt collection and financial litigation records. This notice includes entities with whom, and situations when, DOJ may share data. This notice mitigates the risk of an individual being unaware that information is being collected or how the information will be used.

The TOP 60 day notice informs the individual debtor that their information will be shared with the Department of Treasury for potential offset of benefits, and cites the statute that

requires submission to this program. It also provides the debtor with remedies for preventing the offset from occurring.

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 may make a request for access to or amendment of their records under the Privacy Act and related regulations (28 C.F.R. §§ 16.40-.46), unless the particular records are exempt from the access and amendment provisions. CDCS is exempt from certain provisions of the Privacy Act. The Attorney General has exempted this system from subsections (c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (H) and (I), (e)(5), (e)(8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2) for any criminal information within the system. In addition, the system is exempt pursuant to the provisions of 5 U.S.C. 552a (k)(2) from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H) and (I) and (f).

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

Notice of an individual's rights under the Privacy Act is provided through publication in the Federal Register of a System of Records Notice and in Departmental regulations describing the procedures for making access/amendment requests.

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

During the litigation process, debtors may challenge the validity of a debt. At any time during the collection process they may request a history of payments and a debt balance.

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.

Individuals may make a request for access to or amendment of their records under the Privacy Act and related regulations (28 C.F.R. §§ 16.40-.46) unless the particular records are exempt from the access and amendment provisions. See 7.1. above.

Section 8.0 – Technical Access and Security

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

Cleared and authorized users of CDCS have access to system data. This includes DOJ staff at the U.S. Attorney's Offices, contracted private counsel, staff at six DOJ litigating divisions (Anti-Trust Division, Civil Division, Civil Rights Division, Criminal Division, Environment and Natural Resources Division, Tax Division, Executive Office for U.S. Attorneys, and JMD DCM and OCIO personnel. Additionally, services for the development, maintenance and daily operations of the system are performed under a services contract administered by the DOJ, Justice Management Division. Entities outside of DOJ, including other Federal agencies do not have direct access to CDCS.

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.

There are two contract types that provide for contractor access to the system. The first is a services contract for the development, analysis, and maintenance of the system and the operation of a claim intake and payment processing facility. These contractors work at DOJ sites and access CDCS by logging in to the Justice Consolidated Office Network and then logging in to CDCS. The second contract type provides for individual private counsel firms across the country, which conduct debt collection activities on behalf of DOJ, to access CDCS. Individuals from these firms access CDCS from their offices via the Justice Secure Remote Access (JSRA) network. These JSRA tokens are configured in such a way that the only point on the network that individuals from the firms may access is CDCS. These individuals log in to CDCS with a user ID and password.

CDCS belongs to the DOJ with services (development, analysis, maintenance, etc.) being performed within the scope of a services contract, as indicated above. The system is maintained at JDC within DOJ space. Services performed by the contracted technical team are in accordance with and approved by DOJ employees.

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

Yes. A system user hierarchy was defined and implemented for CDCS users. The hierarchy defines roles based on user’s component, section, location and job function to determine functionality available at each user role.

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

Levels of access are determined by each user's job function (Assistant U.S. Attorney, paralegal, Contract Private Counsel, etc.). Documented Standard Operating Procedures are followed to ensure that each user has only the access necessary to perform his/her job.

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

CDCS access is handled in accordance with applicable DOJ account management policies and procedures, and applicable security controls. Each user account is specific to a particular user. Users roles are audited periodically by the System Security Officer to ensure only valid users have access to the system, and access is assigned according to what was requested. Users who no longer require access to the system are removed immediately.

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

The primary auditing measures and technical safeguards that are in place to prevent misuse of data are associated with access and authentication controls to prevent unauthorized disclosure and subsequent potential misuse of data. The referenced controls are FISMA requirements and are configured in compliance with DOJ Order 2640.2F provisions. These controls include:

- Authenticator/Password management; i.e., application and monitoring of initial distribution, composition, history, compromise, and change of default authenticators in accordance with NIST SP 800-53/IA-5.

- Account Management; i.e., application and monitoring of account establishment, activation, modification, disabling, removal (including unnecessary/defunct accounts) and review, all of which support implementation of "need-to-know" in accordance with NIST SP 800-53/AC-2.

- Access Enforcement; i.e., application and monitoring of access privileges in accordance with NIST SP 800-53/AC-3.
- Least Privilege; i.e., provision of the minimum tools required for a user to perform his/her function in accordance with NIST SP 800-53/AC-6.
- Unsuccessful Login Attempts; i.e., GPSS automatically locks the account until released by a System Administrator when the maximum number of unsuccessful attempt is exceeded in accordance with NIST SP 800-53/AC-7.
- System Use Notification; i.e., a user has to acknowledge Department *policies regarding use before access is granted in accordance with NIST SP 800-53/AC-8.
- Session Lock; i.e., a user has to re-authenticate after a specified period of inactivity in accordance with NIST SP 800-53/AC-11.
- Remote access is controlled and monitored; i.e. encryption is used to protect the confidentiality of remote access sessions through the use of secure remote access tokens in accordance with NIST SP 800-53/AC-11.
- Audit trails are generated to facilitate intrusion detection and identify data misuse. The system is configured to protect audit information and tools from unauthorized access, modification and deletion in accordance with NIST SP 800-53.

.

Additionally, potential risk for unauthorized disclosure of personal information is mitigated by:

- performing background investigations on DOJ and contractor personnel,
- providing initial and annual system security training,
- limiting physical access to the system,
- utilizing least-privilege restrictions based on user role,
- timely installation of security patches,
- monitoring network activity with a continuously monitored Intrusion Detection System,
- encrypting data during remote transmission,
- encrypting data at rest, and
- utilizing separation of duties to limit data 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 DOJ employees and contract staff are required to complete information systems security training annually. A certificate of completion is logged for employees after successful completion of the training. Also, new employees receive training on the use of the system before they are granted access to the system. Users are reminded periodically about Division policies in these areas and of the requirement to comply with these policies.

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

The information is secured in accordance with the DOJ implementation of FISMA requirements as recorded in the JMD, Cyber Security Assessment and Management (CSAM) Certification and Accreditation (C&A) Web solution. Information security complies with the management, operational, and technical controls delineated by NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems. The applied system category control set is **moderate** as defined by NIST Special Publication 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories.

The system was re-certified and accredited (for control compliance as well as adherence to industry security best practices; with a plan for the mitigation of security risks due to technical vulnerabilities) on May 21, 2010.

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

Potential privacy risks may include: (1) possible breach of agency databases; (2) loss or theft of computer equipment; (3) loss or theft of paper documents; and (4) unauthorized disclosure.

Available mitigation efforts include: (1) password protection of electronic data and/or encryption of removable media; (2) physical security and access controls; (3) storage of paper documents in secure facilities and/or locked filing cabinets accessible only to authorized personnel; and (4) notice of potential Privacy Act penalties and or unauthorized disclosure included as part of the CDCS Rules of Behavior signed annually by each user.

In addition, deterrent controls in the form of Warning Banners, Rules of Behavior, Confidentiality Agreements and auditing are in place. Background checks and/or security clearances, coupled with access restrictions, are required for personnel prior to being granted access to system data. Finally, exit procedures for departing employees

and contractors include the prompt disabling of accounts and removal of access rights to all data.

Section 9.0 – Technology

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

Yes. With all acquisitions of new or upgraded hardware, software or other products, a cost-benefit analysis has been performed in accordance with DOJ requirements. IT investments are pursued in accordance with the relevant provisions of the DOJ Systems Development Life Cycle Guidance and Federal Acquisition Regulations.

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

In conformance with DOJ ITSS Standard 2.6, JMD implements data integrity controls to protect data from accidental or malicious alteration or destruction and to ensure that the information is accurate and has not been altered. JMD employs an intrusion detection system to detect vulnerabilities, changes to the network and traffic anomalies. JMD backs up data regularly and controls access to data stored on the GPSS.

9.3 What design choices were made to enhance privacy?

DOJ's security strategy includes protecting all assets from outside attackers as well as from potential internal security violations. To protect personally identifiable and proprietary information, JMD has adopted the incident response plan created by EOUSA in conformance with JMD standards and policy. JMD requires all users to sign General User Rules of Behavior, which address accountability by requiring personnel to protect any and all sensitive information stored or processed by the application. As part of the DOJ infrastructure, JMD employs auditing controls, benefits from the intrusion detection system, secure router configurations, inactivity logouts and firewalls available from the Justice Data Center. All remote access is via Pointsec security software to enhance the security of data. Pointsec complies with Evaluation Assurance Level 4 in Common Criteria quality certification (CC EAL4) and FIPS 140-2.

Conclusion

CDCS processes, stores, and transmits data that supports Department of Justice debt collection activities and related tasks. Securing the information contained in this information system and assuring its proper use is critical to the successful implementation of the Department of Justice financial litigation and debt collection goals.

Every effort is made to ensure that the CDCS architecture complies with the Federal Information Security Management Act, and the Department's implementation of FISMA. To that end, the Program Management team reviews and performs continuous monitoring of the system's technical configuration and operational controls.

DOJ personnel and contractor staff are made aware of their responsibility to properly safeguarding sensitive but unclassified (SBU) data contained in this information system. All users of the system are made aware of specific responsibilities associated with the handling and disclosure of sub-categories of SBU data, including Privacy Act data, Federal Tax Information, and personal identifiable information as appropriate.