The Bureau of the Fiscal Service

Privacy Impact Assessment

The mission of the Bureau of the Fiscal Service (Fiscal Service) is to promote the financial integrity and operational efficiency of the federal government through exceptional accounting, financing, collections, payments, and shared services.

This Privacy Impact Assessment is a Public document and will be made available to the general public via the Fiscal Service Privacy Impact Assessment (PIA) webpage (shown below).

Fiscal Service Privacy - FMS Impact Assessments (PIA): http://www.fms.treas.gov/pia.html

Fiscal Service Privacy – Public Debt Impact Assessments (PIA): http://www.treasurydirect.gov/privacy_impactassessment.htm

Document Date: September 20, 2011

Document Version: 1.0

Name of System: FedDebt

SYSTEM GENERAL INFORMATION:

1) System Overview: Describe the purpose of the system.

The purpose of this system is to maintain records about individuals who owe delinquent non-tax debt(s) to the U.S. Government referred for collection by departmental and program agencies (Creditor Agencies). The information contained in the records is maintained for the purpose of taking action to facilitate the collection and resolution of the debt(s) using various collection methods, including, but not limited to, requesting repayment of the debt by telephone or in writing, offset, administrative wage garnishment, referral to collection agencies, to Department of Justice or for litigation, and other collection or resolution methods authorized or required by law. The information also is maintained for the purpose of providing collection information about the debt to the agency collecting the debt, to provide statistical information on debt collection operations, and for the purpose of testing and developing enhancements to the computer systems that contain the records.

2) Under which Privacy Act Systems of Records Notice (SORN) does the system operate? Provide number and name.

Treasury/FMS.014 Debt Collection Operations System – Treasury/Financial Management Service.

3) If the system is being modified, will the SORN require amendment or revision?

__yes, explain.
X no

4) Does this system contain any personal information about individuals?

X yes
__no

a. Is the information about members of the public?

YES

b. Is the information about employees or contractors?

YES

5) What legal authority authorizes the purchase or development of this system?

In response to a steady increase in the amount of delinquent non-tax debt owed to the United States, Congress passed the Debt Collection Improvement Act (DCIA) of 1996 (Pub L. 104-134, sec. 31001). This law centralized the government-wide administrative collection of non-tax delinquent debt and gave Treasury significant new responsibilities in this area. The

Financial Management Service (FMS) is responsible for Treasury's implementation of the debt collection provisions of the DCIA. The Debt Management Services (DMS), a business line of FMS, is the Government's central debt collection agency. The DCIA requires federal agencies to refer delinquent non-tax debts to FMS for purposes of collection, and FMS to take certain collection actions with respect to the referred debts. The DCIA also authorizes FMS to offset eligible non-tax Federal payments to collect delinquent debts owed to state agencies, including state-enforced delinquent child support obligations. In addition, FMS assists the Internal Revenue Service (IRS) and state agencies in collecting tax debts by withholding eligible Federal payments from delinquent taxpayers, in accordance with the requirements of the Taxpayer Relief Act of 1997 (Pub. L. 105-34) and the Internal Revenue Service Restructuring and Reform Act of 1988 (Pub. L. 105-206). The legal authorities applicable to this system/application are:

- Federal Claims Collection Act of 1966 (Pub L. 89-508), as amended by the Debt Collection Act of 1982 (Pub L. 97-365, as amended) and the Debt Collection Improvement Act of 1996 (noted above), generally codified at 31 U.S.C. 3701 et seq. and 5 U.S.C. 5514.
- Deficit Reduction Act of 1984 (Pub L. 98-369, as amended) (tax refund offset provisions are codified at 26 U.S.C. 6402 and 31 U.S.C. 3720A)
- Treasury's access to information in the National Directory of New Hires (NDNH) is authorized by 42 U.S.C. § 653(j)(9) (as enacted by Public Law No. 108-447, Div. H, Title VI § 643 (Dec. 8, 2004))

DATA in the SYSTEM:

1) **Identify the category of individuals in the system**
   Check all that apply:
   X Employees
   X Contractors
   X Taxpayers
   __Others (describe)

2) **Identify the sources of information in the system**
   Check all that apply:
   X Employee
   X Public
   X Federal agencies
   __ State and local agencies
   X Third party

   a. What information will be collected from employees or contractors?

   Information varies, depending on the individual debtor, the type of indebtedness and the governmental entity to which monies are owed. The system contains information pertaining to:

   - Individuals and commercial organizations, such as name, Taxpayer Identification Number (TIN) (i.e., social security number, or employer identification number), date of birth, work and home address, and work and home phone numbers, financial information, and credit history

   b. What information will be collected from the public?

Information varies, depending on the individual debtor, the type of indebtedness and the governmental entity to which monies are owed. The system contains information pertaining to:

- Individuals and commercial organizations, such as name, Taxpayer Identification Number (TIN) (i.e., social security number, or employer identification number), date of birth, work and home address, and work and home phone numbers, financial information, and credit history

c. What Federal agencies are providing data for use in the system?

The following creditor agencies refer their delinquent non-tax debt for collection:

- Central Intelligence Agency;
- Commodity Futures Trading Commission;
- Consumer Product Safety Commission;
- Corporation for National Service;
- Department of Agriculture:
  - Rural Development Agency,
  - Farm Service Agency,
  - Animal and Plant Health Service,
  - Rural Marketing Agency,
  - National Finance Center,
  - Food and Nutrition Service;
- Department of Commerce;
- Department of Defense:
  - Defense Finance and Accounting Service,
  - Army-Air Force Exchange Service,
  - U.S. Army Community & Family Support Center,
  - Navy Exchange,
  - Navy Personnel Command, Defense Commissary Agency Headquarters,
  - Marine Exchange,
  - Air Force Services;
- Department of Education;
- Department of Energy;
- Department of Health and Human Services:
  - Program Support Center,
  - Office of Child Support Enforcement;
- Department of Homeland Security:
  - Federal Emergency Management Agency,
  - Customs Service,
  - Federal Law Enforcement Training Center,
- Department of Housing and Urban Development;
- Department of the Interior;
- Department of Justice:
  - Bureau of Alcohol, Tobacco and Firearms,
  - Debt Accounting Operations Group;
- Department of Labor;
- Department of State;
- Department of Transportation;

- Department of the Treasury:
  - Financial Management Service - Reclamation Branch,
  - DMS Cross-Servicing,
  - Philadelphia Regional Finance Center,
  - Internal Revenue Service,
  - United States Mint;
  - U. S. Secret Service;
- Department of Veterans Affairs;
- Environmental Protection Agency;
- Equal Employment Opportunity Commission,
- Federal Communications Commission;
- Federal Election Commission;
- Federal Maritime Commission;
- Federal Retirement Thrift Investment Board;
- Federal Trade Commission;
- General Services Administration;
- Government Printing Office;
- James Madison Memorial Fellowship Foundation;
- Library of Congress;
- National Aeronautics and Space Administration;
- National Endowment For The Arts;
- National Indian Gaming Commission;
- National Labor Relations Board;
- National Science Foundation;
- National Security Agency;
- National Transportation Safety Board;
- Nuclear Regulatory Commission;
- Office of Personnel Management;
- Peace Corps;
- Pension Benefit Guaranty Corporation;
- Railroad Retirement Board;
- Securities & Exchange Commission;
- Small Business Administration;
- Social Security Administration;
- U.S. Agency for International Development;
- U.S. House of Representatives;
- U.S. Postal Service.

d. What State and local agencies are providing data for use in the system?

None

e. From what other third party sources will data be collected?

Information in this system is obtained from the individual or entity (or an authorized representative of the individual or entity), Federal agencies, private collection agencies, credit bureaus and other publicly available databases.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources, other than FMS records, be verified for accuracy?

Information collected from the affected individual, entity, or authorized representative, is verified by comparing the information to information collected from Federal agencies that have referred a delinquent debt to FMS for collection and information collected from credit bureaus and other publicly available databases. Individuals, entities, and representatives providing financial information are required to attest to the accuracy of the information.

Federal agencies providing information to FMS are required to certify to FMS as to the accuracy of the information and that all due process pre-requisites to debt collection have been met. Among other things, this means that, prior to submitting the information to FMS, such agencies have sent a notice to the affected individual or entity, to inform the individual or entity about the debt, that the debt will be referred to FMS for collection, and the opportunities available to the individual or entity to dispute the information maintained by the referring agency.

Information provided to FMS by the Department of Health and Human Services (HHS) contains information from the National Directory of New Hires (NDNH), a database of employment information about employed individuals. The NDNH contains the information supplied by each new employee to his or her employer on Internal Revenue Service (IRS) Form W-4 (Employee's Withholding Allowance Certificate) and quarterly wage information provided by employers to state agencies. The employee providing IRS W-4 information declares under penalties of perjury that the information provided (name, TIN, and address) is true, correct, and complete. The quarterly wage information is likewise certified by employers to states as true and correct. HHS provides NDNH information to FMS based on debtor information (name and TIN) provided to HHS by FMS. HHS verifies that a debtor's name and TIN matches an employee's name and TIN in the NDNH. If there is no match, HHS will so notify FMS that the name and TIN do not match the information in the NDNH. HHS supplies only the most recent employment information about a debtor (i.e., employer, employer address, etc.) as is contained in the NDNH, which is updated regularly.

Information obtained by FMS from other publicly available databases is verified by comparing the information to information obtained from other sources before the information is used for purposes of debt collection activities. If an affected individual or entity disputes, in writing, the accuracy of the information contained in the system, FMS will contact the source of the information for additional verification. The credit bureaus that provide information to FMS are subject to the Fair Credit Reporting Act, which provides mechanisms to correct inaccurate information.

b. How will data be checked for completeness?

Data validation and reconciliation checks are performed by Integrated FedDebt during input and export batch processing, and user input. Once a record is created for a Debt/Debtor, the data cannot be deleted in the system. All changes will be appended to the record.

- Input Batch – Incoming files from the various creditor agencies, Federal employing agency, collection agencies, credit bureaus, and Federal, state or local agencies are accepted or rejected based on validation rules for balancing. Syntax checking is limited to only those that are needed for file balancing. The validation program verifies that the file balances and passes other file level edits appropriate for its file type. After the job is run, the Integrated FedDebt validation program issues a successful return code and displays success messages. The program then transmits a copy of a control report to Input Management which will determine further processing based on the return code and the error report. The program saves the file name, job name, processing date, processing time, and return code as log information.
- Output Batch – Integrated FedDebt updates TOP daily. Numerous checks are conducted during the process to ensure that up-to-date data is used when creating the batch file. These checks include: initial referral; adding new debtor to debt; changes to name, address, TIN, amount of debt; etc.
- User Input – Validation checks and lookup tables have been incorporated into the data input screens/fields to help eliminate user input errors.

c. What steps or procedures are taken to ensure the data is current?

The data in the system is the last available information known to the source of the information. Data contained in the system is updated continually with information from the source provider, however not all data records are updated. Data files that have not been updated are placed in an archive in an inactive status. When a file is archived will vary depending on the individual debtor, the type of indebtedness and the governmental entity to which monies are owed.

d. In what document(s) are the data elements described in detail?

Data elements are described and documented in the DMS Data Dictionary. This document may be made available upon request.

ATTRIBUTES OF THE DATA:

1) How is the use of the data both relevant and necessary to the purpose for which the system is being designed?

FedDebt is a debt collection program that DMS utilizes to enforce provisions of the DCIA and other debt collection laws. Records are maintained about individuals who owe delinquent debt(s) to the U.S. Government through one or more of its departments and agencies. The information contained in the records is maintained for the purpose of taking action to facilitate the collection and resolution of the delinquent debt(s) using various collection methods.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected? How will this be maintained and filed?

No. The system will not derive any new data or create previously unavailable data about an individual through aggregation from the information collected as a result of the Integrated FedDebt System. For the purpose of clarity, derive is herein viewed as systemically analyzing the original data, and thereby creating a new or different

category of information. Further, an update to the system is seen as new information (e.g. name change, address), to an existing category or field. This is not new data derived from the system or previously unavailable data created by the system. It is updated information on debtors in the system provided from the individual or entity, creditor agencies, Federal employing agency, collection agencies, skiptrace contractors, and Federal agencies.

Record files on debtors are continually updated based on the data provided from the individual or entity, creditor agencies, Federal employing agency, collection agencies, skiptrace contractors, and Federal agencies, as a matter of standard operating practices. This is the current practice with the debt collection programs in place at DMS and no change to those procedures is planned. FedDebt will only collect, record, and store source information that is received via existing data sources.

The FedDebt program will consolidate data bases currently maintained by other debt collection programs at DMS eliminating potential errors in accounting from duplicate files being maintained on separate data bases.

3) Will the new data be placed in the individual's record?

No. As discussed above in Attributes of the Data No.2., record files on debtors are continually updated based on the data provided from the individual or entity, creditor agencies, Federal employing agency, collection agencies, skiptrace contractors, and Federal agencies, as a matter of standard practices.

4) Can the system make determinations about employees or members of the public that would not be possible without the new data?

No. Debt collection action is based on the information received from the individual or entity, creditor agencies, Federal employing agency, collection agencies, skiptrace contractors, and Federal agencies.

That information is maintained in records on individuals and entities that are financially indebted to the U.S. Government through one or more of its departments and agencies and are the result of participation in a Federal direct or guaranteed loan program, the assessment of a fine, fee, or penalty, an overpayment or advance, or other extensions of credit such as would result from sales of goods or services. Records are also maintained on individuals who are indebted to States, Territories and Commonwealths of the United States, and the District of Columbia.

5) How will the new data be verified for relevance and accuracy?

As detailed in section Attributes of the Data #2., above, no new data is derived from the system nor is there any previously unavailable data created by the system. Information in this system is updated from the individual or entity, creditor agencies, Federal employing agency, collection agencies, skiptrace contractors, and Federal agencies furnishing identifying information and/or address of debtor information. Due to the nature of the information being provided, the data is relevant to the debt collection program. However, because the data is not generated by DMS, it is the responsibility of the source provider to ensure the accuracy of the information provided.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

Level of access to the system is on a need-to-know basis only as authorized by the system owner in accordance with Federal law. Controls are predicated on preventing unauthorized users from accessing FMS IT resources, and to ensure each authorized user is accountable for his actions. These controls are intended to provide for integrity, confidentiality, and availability for FMS IT resources following the least privilege and the separation of duties principles. Procedural and physical safeguards are utilized, such as accountability, receipt records, and specialized communications security. Access to computerized records is limited through the use of access codes, entry logs, and other internal mechanisms, to restrict access to those authorized whose official duties require access. Audit logs are maintained and reviewed. Hard-copy records are held in steel cabinets, with access limited by visual controls and/or lock system. During normal working hours, files are attended by responsible officials; files are locked during non-working hours. The buildings are patrolled by armed uniformed security guards.

Security Awareness, Disclosure Awareness, Privacy Awareness and Cyber Security Awareness training are mandatory training requirements that all FMS employees have to take annually.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? (Explain.)

Yes. Although data and processes are being consolidated, access controls are in place to authorize or restrict the activities of users and system personnel to and within FedDebt. The hardware and software features are designed to permit only authorized access to and within the application, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities. These features are discussed in detail in Access to Data section #1, #2, and #4.

8) How will the data be retrieved? (If personal identifiers are used to retrieve information on the individual, explain and list the identifiers that will be used to retrieve data.)

Records are retrieved by various combinations of name or taxpayer identification number (i.e. social security number or employer identification number), or debt identification number.

9) What kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Reports that contain information regarding debt information; i.e. name, date the debt was incurred, collection attempts, etc. can be generated. These reports would be used by the Federal agency that referred the debt, to facilitate recovery of funds. Access to these reports would be permitted on a need-to-know basis only following the least privilege and the separation of duties principles.

10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses)? How can individuals grant consent?

Individuals do not have the opportunity to decline to provide information because providing information is not voluntary. Information in this system is obtained from Federal agencies, private collection agencies, credit bureaus, and state or local agencies as necessary for debt collection purposes. Amplifying information may be supplied by the individual at their discretion.

Individuals, entities, and representatives providing financial information are required to attest to the accuracy of the information. Federal agencies providing information to FMS are required to certify to FMS as to the accuracy of the information and that all due process pre-requisites to debt collection have been met. Among other things, this means that, prior to submitting the information to FMS, such agencies have sent a notice to the affected individual or entity, to inform the individual or entity about the debt, that the delinquent debt will be referred to FMS for collection, and the opportunities available to the individual or entity to dispute the information maintained by the referring agency.

Information provided to FMS by the Department of Health and Human Services (HHS) contains information from the National Directory of New Hires (NDNH), a database of employment information about employed individuals. The NDNH contains the information supplied by each new employee to his or her employer on Internal Revenue Service (IRS) Form W-4 (Employee's Withholding Allowance Certificate) and quarterly wage information provided by employers to state agencies. The employee providing IRS W-4 information declares under penalties of perjury that the information provided (name, TIN, and address) is true, correct, and complete. The quarterly wage information is likewise certified by employers to states as true and correct. HHS provides NDNH information to FMS based on debtor information (name and TIN) provided to HHS by FMS. HHS verifies that a debtor's name and TIN matches an employee's name and TIN in the NDNH. If there is no match, HHS will so notify FMS that the name and TIN do not match the information in the NDNH. HHS supplies only the most recent employment information about a debtor (i.e., employer, employer address, etc.) as is contained in the NDNH, which is updated regularly.

Information obtained by FMS from other publicly available databases is verified by comparing the information to information obtained from other sources before the information is used for purposes of debt collection activities. If an affected individual or entity disputes, in writing, the accuracy of the information contained in the system, FMS will contact the source of the information for additional verification.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) What are the retention periods of data in this system? How long will the reports produced be kept?

Once an electronic record is created for a Debt/Debtor, the data cannot be deleted in the system unless the data is archived (moved) to another medium for continued preservation or is eligible for destruction based upon a disposition schedule (retention period) approved by the National Archives and Records Administration (NARA). NARA has approved a schedule (N1-425-03-1) for debtor records managed by the Debt Services Division, DMS. Currently, any FMS records that are proposed for destruction must be approved in advance, and in writing, by the FMS Assistant Commissioner for Management and the FMS Chief Counsel, to ensure compliance

with NARA disposition schedules and any record retention orders to which FMS is subject. The FMS Chief Counsel outlined this process in a memorandum to the FMS Assistant Commissioners, dated March 7, 2000.

Summary information, such as results of collection action undertaken, for the purpose of producing management reports is retained for a period of five (5) years. This information does not contain any individual information.

2) What are the procedures for disposition of the data at the end of the retention period? Where are the disposition procedures documented?

Disposition of the data at the end of the retention period, length of time that reports will be kept, and the documentation of the procedures for disposition are discussed in Maintenance and Administrative Controls section #1 above.

3) If the system is operated in more than one site, how will consistent use of the system and data be maintained at all sites?

The system is operated at one site only, the Bureau of the Public Debt, located in Parkersburg, West Virginia.

4) Is the system using technologies in ways that FMS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

Yes. However, while many new technologies will be employed in the Integrated FedDebt Program, the use of these new technologies and their applications relative to the Integrated FedDebt Program do not impact the privacy of information retained in the system with respect to individuals, members of the public, and employees.

5) How does the use of this technology affect employee or public privacy?

As discussed in the Maintenance and Administrative Controls section #4., above, Public/employee privacy will not be affected by the use of new technology in the Integrated FedDebt Program. Additionally, the controls for level of access as noted in the Attributes of The Data section #6., above, will remain in place.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

Yes. This system does provide the capability to identify, locate, and monitor individual users. Treasury policy states that program officials shall ensure users of the IT resources supporting their programs have a validated requirement to access their resources. In support, FMS policy requires the establishment and implementation of account management controls for FMS IT resources. These controls ensure that each authorized user is accountable for his actions and are intended to provide for integrity, confidentiality, and availability for FMS IT resources. These controls are predicated on preventing unauthorized users from accessing FMS IT resources.

Procedural and physical safeguards are utilized, such as accountability, receipt records, and specialized communications security. Access to computerized records is limited through the use of access codes, entry logs, and other internal mechanisms, to restrict access to those authorized whose official duties require access. Audit logs are maintained and will record any access to the data base. The audit logs are reviewed on a daily basis.

These controls afford program officials the ability to identify individuals responsible for inappropriate activity, the location at which the activity took place and the type of activity that took place.

7) What kind of information is collected as a function of the monitoring of individuals?

As a function of monitoring, program officials can determine if the data base was accessed or changed, the type of change, the time of the change, agency, bureau, office, information for each user, and if the user is internal or external. If the user is an external user, information on the agency can be supplied.

8) What controls will be used to prevent unauthorized monitoring?

Monitoring of the Integrated FedDebt system is an automated procedure that is a function of the operating system and several applications. The monitoring is done to produce an audit trail to ensure that all accesses to the system are by authorized personnel following the rules of behavior in performance of official duties. The audit logs are reviewed only by supervisory personnel as determined by the system owner and Information Systems Security Officer (ISSO). Access controls are discussed in greater detail in the Access to Data section #4.

ACCESS TO DATA:

1) Who will have access to the data in the system?
Check all that apply:

X Contractors
X Users
X Managers
X System Administrators
X System Developers
X Others (explain) (Private Collection Agency users, Creditor Agency users and FMS employees)

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

The need for access and the level of access will be validated and verified at a minimum by the system owner in accordance with Federal law, and depending on the IT resource, by the user's supervisor. Information regarding who will have access to the data is provided in the Access to Data section #1., above.

Access controls are the controls in place to authorize or restrict the activities of users and system personnel to and within Integrated FedDebt. The hardware and software features are designed to permit only authorized access to and within the application, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities. The following logical access controls are in place:

- A formal process for requesting, establishing, issuing, and closing user accounts has been established and implemented. All users must apply for access to the Integrated FedDebt system.
- Once the user is approved for access, the Integrated FedDebt system administrator creates the new Integrated FedDebt account. The user is placed in the appropriate group.

- A separation of duties is employed so that an individual is prevented from having the authority or information access to conduct fraudulent activity without collusion with others.
- Integrated FedDebt employs a security environment in which users' rights to access or change information are controlled by the position they fulfill within the organization. Formal procedures are used for defining user authority for both user and privileged accounts. These procedures follow the principle of least privilege, which requires identifying the user's job functions, determining the minimum set of privileges required to perform that function, and restricting the user to those privileges and nothing more.
- Access to the Integrated FedDebt system, the operating system, the databases, and batch accounts used for file transfer purposes are controlled by different applications. These accounts are non-login type accounts and are not accessible for login by anyone.
- Access to computer data is managed by security at the Enterprise level, the application level, and at the database level.
- Integrated FedDebt Access Control Lists (ACLs) are reviewed quarterly to identify and remove users who have left the organization or whose duties no longer require access to the application. User access is deleted within 24 hours of termination of employment or notification of termination of employment. The ACLs are maintained and reviewed on a scheduled basis by the Integrated FedDebt ISSO.
- The system will automatically log off users after 30 minutes of system inactivity.
- Internal and external firewalls have been installed to restrict access. Integrated FedDebt also provides a separate partition to function as the Demilitarized Zone (DMZ) to further protection from public Internet access.
- The system security control functions prohibit public access to Integrated FedDebt and its databases. Only authorized users are identified and authenticated before Web access is granted.

The authorization for access and the level of access allowed in the system will be determined and verified by the system through identification and authentication.

Identification is the means by which a user provides a claimed identity to the system. The following identification controls are in place:

- DMS policy requires a unique user name or user ID be assigned to each user and administrator. External users will access Integrated FedDebt through the Internet using a Web browser and SSL. These users must also provide a unique user ID and password.
- Integrated FedDebt maintains all user records in a security file. Through its auditing capabilities, it can link actions to specific users. Integrated FedDebt maintains the identity of all active users and links actions to specific users at the application level via a number of records through the system functions.
- DMS ensures that all user IDs belong to currently authorized users. Identification data is kept current by adding new and deleting former users.

Authentication is the means of establishing the validity of a user who has claimed identity to the system. There are three means of authenticating a user's identity, which can be used alone or in combination:

- Something the individual knows (a secret – e.g., a password, personal identification number (PIN), or cryptographic key)

- Something the individual possesses (a token – e.g., an ATM card or a smart card)
- Something the individual is (a biometrics – e.g., characteristics such as a voice pattern, handwriting dynamics, or a fingerprint)

Authentication controls in place for Integrated FedDebt include but are not limited to:

- Passwords are at least eight characters in length and contain a mixture of uppercase and lowercase letters, and a numeric or special character
- Common user passwords expire after 90 days and privileged users expire after 30 days

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

Users will not have access to all the data on the system. User level of access is restricted to a need-to-know basis only following the least privilege and the separation of duties principles.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)

Users having access to the data in the system are subject to the Privacy Act, applicable laws governing access to information in the National Directory of New Hires (NDNH), taxpayer disclosure laws, other applicable laws, regulations, and policies, and the Rules of Behavior signed by each user.

System controls are predicated on preventing unauthorized users from accessing DMS IT resources and ensuring each authorized user is accountable for his actions. These controls are intended to provide for integrity, confidentiality, and availability for DMS IT resources following the least privilege and the separation of duties principles.

FMS has specific procedures in place for evaluating the sensitivity and access levels required for staff and contractor positions. Individuals associated with FMS systems receive the background screening appropriate for the position to which they are assigned via the federal employment suitability process. Access may be granted to users after completing and submitting the required background screening forms (e.g., SF-85/85P). Additionally, mechanisms have been formally implemented, such as signatures on the Rules of Behavior, to hold users accountable for their actions. Creditor agencies, fiscal agents, and contractors must comply with the requirements of applicable laws, regulations, and agreements; contractor personnel must sign confidentiality agreements.

Security awareness and training provide system users with the context and methods needed to use the system securely and to protect sensitive equipment and data. FISMA requires FMS to provide mandatory periodic training in computer security awareness, including accepted computer security practice, for all employees and contractors who are involved with the management, use, or operation of FMS computer systems. OMB Circular A-130, Appendix III, reissued in November 2000, enforces mandatory training by requiring its completion prior to granting access to the system and through periodic refresher training for continued access. Therefore, each user must be versed in acceptable Rules of Behavior for FMS and Integrated FedDebt before being allowed access. The training program also informs users how to obtain help when

having difficulty using the system and educates them on procedures for reporting security incidents.

FMS security policies and procedures are available to all FMS employees on the FMS intranet site at http://intranet.fms.treas.gov/. The Security Awareness Training and Education (SATE) program at FMS includes a formal security training process. Signed disclosure forms and statements by users are maintained by the FMS Security Branch to indicate each trainee's participation. Documentation of the content of the SATE program is maintained and updated. Mandatory security awareness and threat training is conducted annually. New users are required to complete security awareness training and sign the Rules of Behavior within 30 days of gaining system access, and annually thereafter. Contractor and fiscal agent personnel are required to receive the same level of automated information system security awareness and training as federal employees. Formal and informal Integrated FedDebt-specific training is provided for new users and contractor and fiscal agent personnel. As part of the security program, periodic reminders are distributed in the form of e-mails, calendars, mouse pads, mugs, and pens. Additionally, FMS encourages employees to obtain specialized training and achieve technical certifications.

Audit logs are maintained and will record any access to the data base. A description of the in-place Integrated FedDebt auditing methods and procedures is as follows:

- An audit trail is created each time a user logs onto Integrated FedDebt. User IDs and the time of log on/off are captured and stored in the audit trail log. All specified changes to data (e.g., add, update, as well as, who made the changes, what the changes were, and when the changes occurred) are captured and stored. The operating systems capture all system administrators' accesses to root and the data base management system
- Sufficient information is collected to support after-the-fact investigations of how, when, and why normal operations ceased. Logs, audit trails, and managerial supervision all ensure that employees are held accountable for their actions
- Access to online Integrated FedDebt audit logs is strictly controlled, as is access to audit logs removed from the system and stored on paper or electronic media
- Integrated FedDebt audit logs are stored indefinitely. Access to the logs in storage is limited to authorized personnel
- Electronic audit trails are created as receipt of inputs/outputs to and from the Integrated FedDebt system
- System security will review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem
- The audit logs are reviewed on a daily basis
- Auditing tools are available to view audit trails in real-time, or near real-time

5) If contractors are/will be involved with the design, development or maintenance of the system were Privacy Act contract clauses inserted in their contracts and were other regulatory measures addressed?

Yes, contractor personnel are involved in the design and development of the system but do not have access to any sensitive personal information contained in the data system. In the remote circumstance that a contractor should require access to personal

information, the Director, Acquisition Management Division, in consultation with the Disclosure Officer and the Office of Chief Counsel, will ensure that all FMS contracts include provisions, where appropriate, outlining the contractor's responsibilities with regard to the use of personal information obtained from DMS. These provisions may include a requirement that the contractor provide training to those contractor employees working on the contract with access to personal information. Prior to requesting contracting assistance from the Acquisition Management Division, each program area, in consultation with that area's Privacy Act Liaison Officer, will identify whether or not the contract will involve access to and use of personal information.

It should also be noted that the primary design, development, and maintenance of the Integrated FedDebt Program will be accomplished by the FRB as the fiscal agent for FMS. Integrated FedDebt will utilize custom development and integration of existing DMS systems. SFFRB resources will be utilized to perform custom development. SFFRB was intimately involved in the very successful development of the TOP.

The relationship between FMS and the FRB is unique and guided by statutory authority dating back to 1913. The FRB is not a client, contractor, or customer to FMS, but a fiscal agent. DMS directs the FRB, as the fiscal agent for FMS, to develop and implement solutions (including IT) that are beneficial to the Government.

While the FRB is not considered as a client, contractor, or customer to FMS, FRB personnel are subject to the Privacy Act, applicable laws governing access to information in the National Directory of New Hires (NDNH), taxpayer disclosure laws, other applicable laws, regulations, and policies, and the Rules of Behavior signed by each user.

6) Do other systems share data or have access to the data in the system?

X yes
__no

If yes,

a. Explain the interface.

Yes. Integrated FedDebt has major interfaces with:

- Creditor Agencies - Batch files are provided for entry of new delinquent debts into the Integrated FedDebt system as well as for updating of existing debt/debtor information. Debts can be recalled from collection by the creditor agency or can be returned to the agency from Integrated FedDebt as uncollectible.
- Private Collection Agencies (PCAs) - New delinquent debts are assigned and distributed to the PCAs. Updates of debt/debtor information and updated accounting information for cases are also forwarded to the assigned PCAs. Updates of debt/debtor information can also be forwarded to Integrated FedDebt when identified by the PCAs. Debts can be recalled from a PCA collection or can be returned by a PCA as uncollectible.
- Treasury Offset Program (TOP) – Debt updates are sent via batch file from FedDebt to TOP and TOP collections are sent via batch file from TOP to FedDebt to update debts in FedDebt.

- Financials, Accounting, Collections, Disbursements, and Reconciliations (FACDR) - This system uses the Oracle Federal Financials application to track, post, and report the accounting activity for delinquent debt collections.

Integrated FedDebt also interfaces with the Department of Health and Human Services (HHS), Office of Child Support Enforcement (OCSE) for the National Directory of New Hires (NDNH) by providing an extract file that contains individual identifying information (name and TIN) about debtors to OCSE, which in turn provides employment information about those debtors to Integrated FedDebt. The information contained in the extract file provided by FMS is not retained by the OCSE.

b. Identify the role responsible for protecting the privacy rights of the public and employees affected by the interface.

The FMS Office of the Chief Information Officer (CIO), FMS Information Systems Security Officer (ISSO), and FMS Business Line Executives all work together to protect the privacy rights of the public.

7) Will other agencies share data or have access to the data in this system?

X yes
__no

If yes,

a. Check all that apply:

X Federal
__State
__Local
X Other (explain) __Private Collections Agencies_____

b. Explain how the data will be used by the other agencies.

Other agencies will use the data to facilitate the collection of delinquent debt and update records of debtors.

Other agencies will have access to the data and share data with the Integrated FedDebt system; however, any other agency will have access only to the data that is relevant to that agency for the collection of its delinquent debt. Data in the system supplied by HHS from the NDNH will be available in view access only to authorized DMS personnel and to the PCA that is assigned collection activity. NDNH data will not be shared with other creditor agencies nor will they have access to the data obtained from the NDNH.

c. Identify the role responsible for assuring proper use of the data.

FMS (through its DMS business line) has primary responsibility for assuring proper use of the data in the Integrated FedDebt System. However, other Federal agencies and private collection agencies all share responsibility for ensuring proper use of the data to which their employees have access. Credit bureaus are required to follow federal law, including the Fair Credit Reporting Act (FCRA) to ensure proper use of the data reported to them from the Integrated FedDebt System.