



Privacy Impact Assessment

For

Financial Management System (FMS)

Date:

January 6, 2011

Point of contact:

(Daniel Dytang, 202-377-3431, Daniel.Dytang@ed.gov)

System Owner:

(Milton L. Thomas Jr., 202-377-3182, Milton.Thomas@ed.gov)

Author:

(Steven Sarmiento, 202-377-3644, Steven.Sarmiento@ed.gov)

**Office of Federal Student Aid
U.S. Department of Education (ED)**

1. System Information. Describe the system - include system name, system acronym, and a description of the system, to include scope, purpose and major functions.

FMS is an integrated financial management system, utilizing Oracle Federal Financials, which incorporates full financial business functionality, including general ledger (GL), accounts payable (AP), and accounts receivable (AR,) across multiple FSA program areas.

FMS supports the FSA Chief Financial Officer's (CFO) directive to account for all FSA program transactions including, but not limited to, the Federal Family Education Loan (FFEL) Program, the Federal Pell Grant Program, and the William D. Ford Federal Direct Loan (Direct Loan) Program; to perform funds checking; and to support the Department of Education's financial statements. FMS is the single point of institutional financial information for FSA, integrating data from several sources. This includes transactions both from the FSA Title IV systems such as eCampus-Based (eCB), Common Origination and Disbursement (COD), as well as from the Department's Education Central Automated Processing System (EDCAPS), which includes, among other systems, the Grants Administration Payment System (GAPS) and Financial Management System Software (FMSS). Accordingly, FMS provides AR, AP, and GL data to support key management analysis and is the only place within the Department of Education that provides a comprehensive financial picture of a school across all FSA programs. This data is used to support the operations of various FSA programs such as, but not limited to, the Federal Family Education Loan (FFEL) Program, Leveraging Educational Assistance Partnership/Special Leveraging Educational Assistance Partnership (LEAP/SLEAP), and various Title IV programs.

FMS maintains Privacy Act records and discloses records to both the U. S. Department of the Treasury and to loan holders. FSA categorizes FMS as an official system of records under the Privacy Act.

One of the primary objectives of FMS is to provide the necessary technical interfaces in order to be fully operational with other FSA information systems. For this reason, interfaces to the FMS application constitute a major portion of the system activity. FMS has customized interfaces, or "extensions," that provide additional functionality to FMS. These extensions include LEAP/SLEAP, Lender Reporting System (LaRS), Lender's Application Process (LAP), and the Guaranty Agency Financial Report – Form 2000 (OMB Control Number 1845-0026. These extensions allow for the collection of data from financial partners in the FFEL program and the LEAP/SLEAP program.

2. Legal Authority. Cite the legal authority to collect and use this data. What specific legal authorities, arrangements, and/or agreements regulate the collection of information?

20 U.S.C. 1070 *et seq.* Title IV of the Higher Education Opportunity Act (HEOA) (Public Law 110-315) enacted on August 14, 2008, which reauthorizes the Higher Education Act of 1965, as amended (HEA).

ECASLA of 2008 (Public Law 110-227) and 31 U.S.C. 7701 and Executive Order 9397 (November 22, 1943), as amended by Executive Order 13478 (November 18, 2008).

3. Characterization of the Information. What elements of Personal Identifiable Information (PII) are collected and maintained by the system (e.g., name, social security number, date of birth, address, phone

number, etc.)? What are the sources of information (e.g., student, teacher, employee, university)? How the information is collected (website, paper form, on-line form)? Is the information used to link or cross-reference multiple databases?

Records in the FMS system include, but are not limited to, (1) personally identifiable information (PII) about individual borrowers who are entitled to a refund of loan overpayment or loan discharge, and information received as loan servicing financial records. Loan refund information includes a borrower's Social Security Number (SSN), name and address, amount of overpayment to be refunded, and name of the loan holder and bank account information. Financial records received from Title IV servicers and Ensuring Continued Access to Student Loans Act (ECASLA) custodians contain the SSN of the borrowers used specifically for the accounting of loans.

FMS does not collect any data directly from users, but stores PII data as it is received from other FSA, contractor-managed systems; and trading partner systems; as well as organizations that support title IV programs. The list below provides an example of the systems with whom FMS exchanges data, but is not limited to these systems:

- (a) Common Origination and Disbursement (COD) System,
- (b) Direct Loan Consolidation System (DLCS),
- (c) Direct Loan Servicing System (DLSS),
- (d) Debt Management and Collection System (DMCS),
- (e) eCampus Based System (eCBS),
- (f) Department's Education Central Automated Processing System (EDCAPS), which includes the Grants Administration Payment System (GAPS) and Financial Management System Software (FMSS),
- (g) Financial Partner Data Mart (FPDM),
- (h) National Student Loan Data System (NSLDS),
- (i) Postsecondary Education Participants System (PEPS),
- (j) Student Aid Internet Gateway (SAIG) mailboxes,
- (k) Affiliated Computer Services (ACS),
- (l) Title IV Additional Servicers (TIVAS), and
- (m) Loan-servicing companies, financial agencies, Federal, State, and local government agencies, and institutions of higher education.

4. **Why is the information collected? How is this information necessary to the mission of the program, or contributes to a necessary agency activity.** Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The information contained in this system is maintained for the following purposes relating to students and borrowers: (1) to determine student/borrower eligibility for refunds of loan overpayments or loan discharges received by the Department's Office of Federal Student Aid from individual borrowers participating in the title IV, HEA programs; (2) to report information for the purpose of processing refunds to borrowers or loan holders (lenders and guaranty agencies) for overpayments and discharges of title IV, HEA, federal student aid; (3) to receive loan refund information and to send refund transaction data files (the borrower's name and other identifiers) to the Department of Education's Central Automated Processing System (EDCAPS) for validation and subsequent payment by the Department of the Treasury to the borrower; and (4) to receive financial records from title IV servicers

and Ensuring Continued Access to Student Loans Act (ECASLA) custodians that contain SSNs of the borrowers used specifically for the accounting of loans.

Access to FMS is granted only to authorized Department employees, contractors, and trading partners. FMS users are required to submit to a security background check and to obtain a minimum 5C background clearance to obtain access to privacy information. Also, security rules are implemented within FMS that restrict access to view PII data to only those users with a need-to-know to perform their particular job functions. All individuals who apply for FMS access must review and sign a Rules of Behavior and Privacy Act Statement in order for a user account to be created. All users who access the FMS application receive an approved Government System warning prompt each time they enter FMS. The general public is not allowed access to the FMS system. The Virtual Data Center and the General System Support provider, where the FMS application is hosted, provide a comprehensive set of management, operational, and technical security controls in accordance with NIST Special Publication 800-53, Revision 3, "Recommended Minimum Security Controls for Federal Information Systems and Organizations," and meet all the requirements of the Federal Information Security Management Act of 2002. These security controls include, but are not limited to, physical and environmental protection; personnel security; awareness and training; auditing and periodic risk assessments and security authorizations; policies and procedures; and technical controls such as firewalls, identification and authentication and other logical access controls, intrusion detection systems, and regularly scheduled vulnerability scanning and security software updates. The Oracle application provides FMS with the ability to restrict access to the database and operating system. FMS uses strong encryption algorithms for communications between the application and the Oracle Database to ensure that data are encrypted and protected while in transit. Within the Oracle application, personal information, (e.g., the borrower's name and SSN) is embedded in tables that are accessible only through database query tools. Access is restricted by FMS based on the user's role and responsibility within the organization.

Privacy risks of unauthorized disclosure of PII are mitigated by limiting access to FMS and, when appropriate, sanitizing the information once the transaction validation is completed. All users of this system of records are given a unique user identification and are required to establish a password that adheres to the Federal Student Aid Information Security and Privacy Policy (this policy requires a complex password that must be changed every 90 days). Annually, all users of FMS must acknowledge the completion of FMS-specific security awareness training before they can obtain or renew their access to the system. An automated audit trail documents user activity of each person and device having access to FMS.

ED Directive OM: 6-104, The Privacy Act of 1974 (The Collection, Use, and Protection of Personally Identifiable Information) provides for disciplinary actions, civil and criminal penalties as follows " All ED employees and contractors have responsibilities to prevent the improper disclosure of records that are subject to the Privacy Act. Willful violation of the Privacy Act can result in criminal sanctions against an employee or contractor and civil liability for ED and its contractors". This policy is also included as part of the required annual security awareness training.

5. Social Security Numbers - If an SSN is collected and used, describe the purpose of the collection, the type of use, and any disclosures. Also specify any alternatives that you considered, and why the alternative was not selected. **If system collects SSN, the PIA will require a signature by the Assistant Secretary or designee. If no SSN is collected, no signature is required.**

FMS does not collect any data directly from users, but stores PII data as it is received from other FSA, contractor-managed, and trading partner systems that support Title IV programs for the following purposes relating to students and borrowers: (1) to determine student/borrower eligibility for refunds of loan overpayments or loan discharges received by the Department's Office of Federal Student Aid from individual borrowers participating in the title IV, HEA programs; (2) to report information for the purpose of processing refunds to borrowers or loan holders (lenders and guaranty agencies) for overpayments and discharges of title IV, HEA, federal student aid; (3) to receive loan refund information and to send refund transaction data files (the borrower's name and other identifiers) to the Department of Education's Central Automated Processing System (EDCAPS) for validation and subsequent payment by the Department of the Treasury to the borrower; and (4) to receive financial records from title IV servicers and Ensuring Continued Access to Student Loans Act (ECASLA) custodians that contain SSNs of the borrowers used specifically for the accounting of loans.

The Department may disclose information contained in FMS under the routine uses listed in this system of records without the consent of the individual if the disclosure is compatible with the purposes for which the record was collected. These disclosures may be made on a case-by-case basis or, if the Department has complied with the computer matching requirements of the Privacy Act of 1974, as amended, under a computer matching agreement:

- (1) Program Disclosures
- (2) Freedom of Information Act (FOIA) or Privacy Act Advice Disclosure
- (3) Disclosure to the DOJ
- (4) Contract Disclosure I
- (5) Litigation and Alternative Dispute Resolution (ADR) Disclosures
- (6) Research Disclosure
- (7) Congressional Member Disclosure
- (8) Disclosure for Use by Other Law Enforcement Agencies.
- (9) Enforcement Disclosure
- (10) Employment, Benefit, and Contracting Disclosure
- (11) Employee Grievance, Complaint or Conduct Disclosure
- (12) Labor Organization Disclosure
- (13) Disclosure in the Course of Responding to a Breach of Data
- (14) Disclosure to the OMB for Credit Reform Act (CRA) support
- (15) Disclosures to third-parties through computer matching programs

6. **Uses of the Information.** **What is the intended use of the information?** How will the information be used? Describe all internal and/or external uses of the information. What types of methods are used to analyze the data? Explain how the information is used, if the system uses commercial information, publicly available information, or information from other Federal agency databases.

Information in FMS is used for the purpose of processing refunds to borrowers or loan holders (lenders and guaranty agencies) for overpayments and loan discharges of Title IV federal student aid. FMS receives loan refund information and sends refund transaction data files (the borrower's name and other identifiers) to the Department of Education's Central Automated Processing System (EDCAPS) for validation and subsequent payment by the Department of the Treasury to the borrower.

Records in this system are retrievable by name of borrower and address. Full FMS application functionality is available for FMS users through ED's internal network or a virtual private network. Limited FMS application functionality is available to authorized trading partners via an external facing web server, but each can view or submit only their own data. Title IV Additional Servicers (TIVAS) are allowed to view reports containing PII data for general ledger work-in-progress (WIP) and account Transfers In and Out transactions between servicers, but only for transactions they initiate or for which they are directly assigned.

7. Internal Sharing and Disclosure. With which internal ED organizations will the information be shared? What information is shared? For what purpose is the information shared? Describe the risks to privacy for internal sharing and disclosure and describe how the risks were mitigated.

FMS exchanges data with the following internal ED organizations (note: the list below is not all-inclusive):

- (a) Common Origination and Disbursement (COD) System,
- (b) Direct Loan Consolidation System (DLCS),
- (c) Direct Loan Servicing System (DLSS),
- (d) Debt Management and Collection System (DMCS),
- (e) eCampus Based System (eCBS),
- (f) Department's Education Central Automated Processing System (EDCAPS), which includes the Grants Administration Payment System (GAPS) and Financial Management System Software (FMSS),
- (g) Financial Partner Data Mart (FPDM),
- (h) National Student Loan Data System (NSLDS),
- (i) Postsecondary Education Participants System (PEPS),
- (j) Student Aid Internet Gateway (SAIG) mailboxes, and
- (k) Title IV Additional Servicers (TIVAS)

Information in FMS is used for the purpose of processing refunds to borrowers or loan holders (lenders and guaranty agencies) for overpayments and loan discharges of Title IV federal student aid. FMS receives loan refund information and sends refund transaction data files (the borrower's name and other identifiers) to the Department of Education's Central Automated Processing System (EDCAPS) for validation and subsequent payment by the Department of the Treasury to the borrower.

Privacy risks of internal unauthorized disclosure of PII are mitigated by limiting access to FMS and, when appropriate, sanitizing the information once the transaction validation is completed. All users of this system are given a unique user identification and are required to establish a password that adheres to the Federal Student Aid Information Security and Privacy Policy (this policy requires a complex password that must be changed every 90 days). Annually, all users of FMS must acknowledge the completion of FMS-specific security awareness training before they can obtain or renew their access to the system. An automated audit trail documents user activity of each person and device having access to FMS.

ED Directive OM: 6-104, The Privacy Act of 1974 (The Collection, Use, and Protection of Personally Identifiable Information) provides for disciplinary actions, civil and criminal penalties as follows " All ED employees and contractors have responsibilities to prevent the improper disclosure of records that

are subject to the Privacy Act. Willful violation of the Privacy Act can result in criminal sanctions against an employee or contractor and civil liability for ED and its contractors". This policy is also included as part of the required annual security awareness training.

8. **External Sharing and Disclosure.** With what external entity will the information be shared (e.g., another agency for a specified programmatic purpose)? What information is shared? For what purpose is the information shared? How is the information shared outside of the Department? Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU) or other type of approved sharing agreement with another agency? Describe the risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

FMS exchanges data with the following external organizations (note: the list below is not all-inclusive):

- (a) Affiliated Computer Services (ACS),
- (b) Loan-servicing companies,
- (c) Financial agencies,
- (d) Federal, state, and local government agencies,
- (e) Institutions of higher education, and
- (f) The U.S. Department of Treasury

FMS receives this information to conform to the standard Department of Treasury check/EFT layout (SF 1166 format) requirements for refund payment processing. The Department of Treasury may use the refund information in pursuing offsets against obligations owed to the Federal Government.

FMS does not currently have a MOU, contract, or agreement in place describing safeguards, training, access controls, and security measures with the Department of Treasury.

Privacy risks of external unauthorized disclosure of personally identifiable information are mitigated by limiting access to the FMS and when appropriate, sanitization of the information once transaction validation is completed. This system of records limits data access to Department and contract staff on a need-to-know basis and controls individual users' ability to access and alter records within the system. The FMS application is only accessible through the Department of Education internal network or authorized VPN users. Access to FMS is granted only to authorized Federal Student Aid employees, contractors, and partners. FMS users are required to pass a security background check and to obtain a minimum 5C clearance to obtain access to privacy information. Also, security rules are implemented within FMS that restrict access to view PII data only to users with a need-to-know to perform their particular job functions.

All users of this system of records are given a unique user identification and are required to establish a password that adheres to the Federal Student Aid Information Security and Privacy Policy requiring a complex password that must be changed every 60–90 days in accordance with Department information technology standards. Annually, all users of FMS must acknowledge the completion of FMS specific security awareness training before they can obtain or renew their access to this system of records. An automated audit trail documents the identity of each person and device having access to FMS.

ED OM:6-104, The Privacy Act of 1974 (The Collection, Use, and Protection of Personally Identifiable Information), outlines the disciplinary civil actions and criminal penalties as follows “ All ED employees and contractors have responsibilities to prevent the improper disclosure of records that are subject to the Privacy Act. Willful violation of the Privacy Act can result in criminal sanctions against an employee or contractor and civil liability for ED and its contractors”.

This policy is also included as part of the annual security awareness training required.

9. **Notice.** Is a notice provided to the individual prior to collection of their information (e.g., a posted Privacy Notice)? What opportunities do individuals have to decline to provide information (where providing the information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

Because FMS does not collect any personally identifiable information directly from any public end user, FMS does not provide a privacy notice to individuals about whom it collects PII. No opportunities are provided to individuals to consent to the uses of their information in this system.

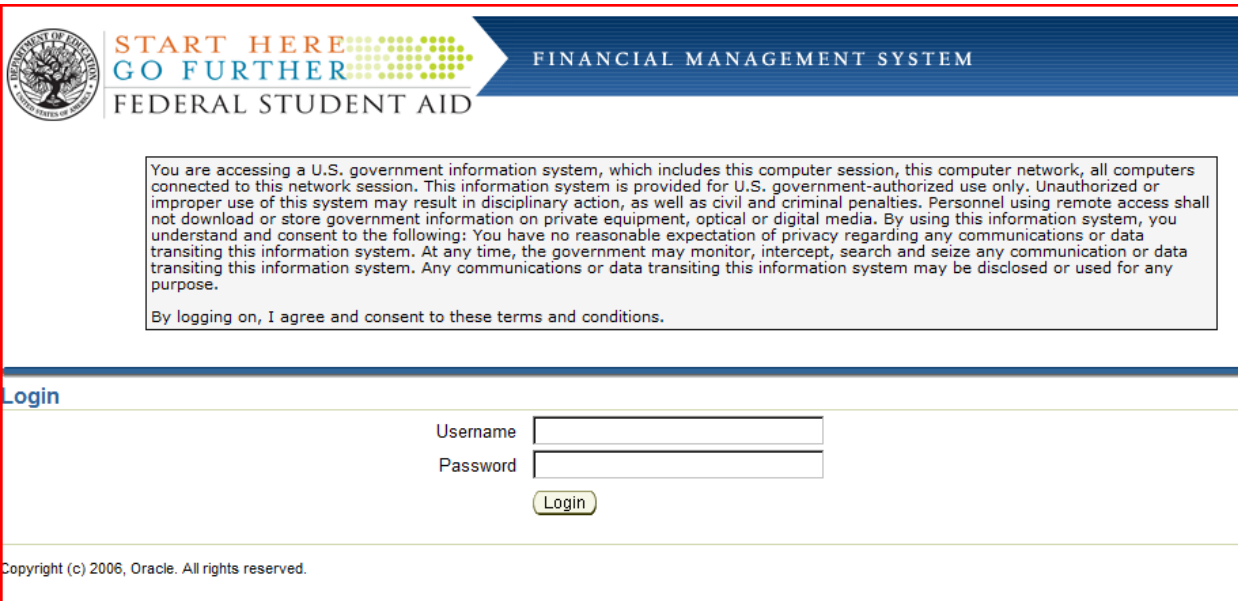
10. **Web Addresses.** List the web addresses (known or planned that have a Privacy Notice.

FMS is not a publicly accessible system, and is accessible only by authorized internal users, and external partners.

As the system is not publicly accessible, and does not collect any personally identifiable information directly from any public end user, FMS is exempt from placing a privacy notice on the website. In accordance with OMB Memo M-03-22, Attachment A, Section III (C), dated September 26, 2003, FMS is excluded as the guidance does not apply to “agency intranet websites that are accessible only by authorized government users (employees, contractors, consultants, fellows, grantees).”

11. **Security.** What administrative, technical, and physical security safeguards are in place to protect the PII? Examples include: monitoring, auditing, authentication, firewalls, etc. Has a Certification and Accreditation (C&A) been completed? Is the system compliant with any federal security requirements? If so, which federal security requirements?

Access to FMS is granted only to authorized Department employees, contractors, and trading partners. FMS users are required to submit to a security background check and to obtain a minimum 5C background clearance to obtain access to privacy information. Also, security rules are implemented within FMS that restrict access to view PII data to only those users with a need-to-know to perform their particular job functions. All individuals who apply for FMS access must review and sign a Rules of Behavior and Privacy Act Statement in order for a user account to be created. All users who access the FMS application receive an approved Government System warning prompt each time they enter FMS.



**START HERE
GO FURTHER**
FEDERAL STUDENT AID

FINANCIAL MANAGEMENT SYSTEM

You are accessing a U.S. government information system, which includes this computer session, this computer network, all computers connected to this network session. This information system is provided for U.S. government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties. Personnel using remote access shall not download or store government information on private equipment, optical or digital media. By using this information system, you understand and consent to the following: You have no reasonable expectation of privacy regarding any communications or data transiting this information system. At any time, the government may monitor, intercept, search and seize any communication or data transiting this information system. Any communications or data transiting this information system may be disclosed or used for any purpose.

By logging on, I agree and consent to these terms and conditions.

Login

Username

Password

Login

Copyright (c) 2006, Oracle. All rights reserved.

The general public is not allowed access to the FMS system. The Virtual Data Center and the General System Support provider, where the FMS application is hosted, provide a comprehensive set of management, operational, and technical security controls in accordance with NIST Special Publication 800-53, Revision 3, “Recommended Minimum Security Controls for Federal Information Systems and Organizations,” and meet all the requirements of the Federal Information Security Management Act of 2002. These security controls include, but are not limited to, physical and environmental protection; personnel security; awareness and training; auditing and periodic risk assessments and security authorizations; policies and procedures; and technical controls such as firewalls, identification and authentication and other logical access controls, intrusion detection systems, and regularly scheduled vulnerability scanning and security software updates. The Oracle application provides FMS with the ability to restrict access to the database and operating system. FMS uses strong encryption algorithms for communications between the application and the Oracle Database to ensure that data are encrypted and protected while in transit. Within the Oracle application, personal information, (e.g., the borrower’s name and SSN) is embedded in tables that are accessible only through database query tools. Access is restricted by FMS based on the user’s role and responsibility within the organization.

Privacy risks of unauthorized disclosure of PII are mitigated by limiting access to FMS and, when appropriate, sanitizing the information once the transaction validation is completed. All users of this system of records are given an unique user identification and are required to establish a password that adheres to the Federal Student Aid Information Security and Privacy Policy (this policy requires a complex password that must be changed every 90 days). Annually, all users of FMS must acknowledge the completion of FMS-specific security awareness training before they can obtain or renew their access to the system. An automated audit trail documents user activity of each person and device having access to FMS.

ED OM: 6-104, The Privacy Act of 1974 (The Collection, Use, and Protection of Personally Identifiable Information) provides for disciplinary actions, civil and criminal as follows “ All ED employees and contractors have responsibilities to prevent the improper disclosure of records that are subject to the Privacy Act. Willful violation of the Privacy Act can result in criminal sanctions against

an employee or contractor and civil liability for ED and its contractors”. This policy is also included as part of the required annual security awareness training.

12. Privacy Act System of Records. Is a system of records being created or altered under the Privacy Act, 5 U.S.C. 552a? Is this a Department-wide or Federal Government-wide SORN? If a SORN already exists, what is the SORN Number?

In accordance with 5 U.S.C. 552a(e)(4) and (11), FSA has published a System of Records Notice of the Financial Management System (FMS) in the Federal Register. The SORN may be located at: 73 Federal Register 177 – 179, (January 2, 2008) or at <http://www.ed.gov/notices/pai/pai-18-11-17.pdf>. The FMS has submitted an updated Notice of an Altered SORN that is currently being reviewed by the Department’s Policy Liaison and Implementation division and the Office of General Counsel. This PIA is consistent with the recently submitted Notice of an Altered SORN.

For general questions please contact: (FMS ISSO-Daniel Dytang, 202-377-3431, Daniel.Dytang@ed.gov)

For privacy issues please contact: Stan Niles, (202-377- 4830), FSA Chief Information Security Officer (CISO) & Chuck Tobler, (202-377- 3472), FSA Privacy Advocate, Department of Education, Federal Student Aid, Washington, D.C. 20528.

13. Records Retention and Disposition. Is there a records retention and disposition schedule approved by the National Archives and Records Administration (NARA) for the records created by the system development lifecycle AND for the data collected? If yes – provide records schedule number:

FMS’ records retention and disposal schedule is in compliance with the Department’s Records Retention and Disposition Schedule (RRDS) policy and the guidance specified by the National Archives and Records Administration (NARA). The FMS is covered by ED 069 Financial Management System, Item a, which is pending approval from the NARA. The retention is: Cut off annually when entity ceases participation in Title IV programs. Destroy/delete 15 years after cut off. The FMS also utilizes ED 086 Information Systems Supporting Materials, Items a, b, and d; which follows General Records Schedule (GRS) 20 items 2, 10, and 11.