Privacy Impact Assessment
For
Management Information System (MIS)

Date:
September 4, 2015

Point of contact:
Hui Yang
hui.yang@ed.gov

System Owner:
Wanda Scott
wanda.scott@ed.gov

Author:
Oscar Rosario
oscar.rosario@ed.gov

Office of the Inspector General (OIG)

U.S. Department of Education (DoED)

1. **System Information. Describe the system -** Indicate whether the system is new or existing and whether or not the PIA is new or being updated from a previous version; specify whether the system is "agency" or "contractor.".

The Office of Inspector General Management Information System (MIS) is a suite of applications used by OIG staff to perform functions related to audits, budget, correspondence, Freedom of Information Act (FOIA) requests, training, and human resources (HR). This is a new Privacy Impact Assessment for a pre-existing operational system. MIS uses a client/server framework with a Visual Basic front end (the client) and a Microsoft SQL Server database backend. Within MIS, only the Human Resources (HR) and Budget Control System (BCS) applications contain Personally Identifiable Information (PII). MIS is hosted on EDUCATE (Education Department Utility for Communications, Applications and Technology Environment) at a contractor (Dell) facility. The EDUCATE PIA can be found at http://www2.ed.gov/notices/pia/educate_102809.pdf.

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

5 U.S.C. Appendix § 6(a)(7), Inspector General Act of 1978, as amended.

3. **<u>Characterization of the Information</u>. 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 is the information collected (website, paper form, on-line form)? Is the information used to link or cross-reference multiple databases?**

The following PII elements are maintained in the MIS application for employees: name, date of birth, Social Security Number (SSN), grade, step, salary, home telephone number, cellular telephone number, race, and national origin identifier.

The following PII elements are collected and maintained in the MIS application for contractors: name, address, home, and cellular telephone number.

The following information is maintained for employees and contractors: emergency point of contact's name, phone number, and relationship to employee or contractor (e.g., spouse, parent, etc.).

For employees, the source of the PII is the Department of Education (Department) Federal Personnel Payroll System known as FPPS Datamart.

The data is updated by executing a database script that updates the OIG MIS database with the most current data from FFPS Datamart.

The information is not linked or cross-referenced in other databases.

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.**

PII is used to process personnel actions including promotions, step increases, buy-outs, and retirements. It is also used for retirement calculations and other budget related purposes. Emergency contact information is collected for purposes of continuity of operations, contingency plan, and OIG personnel emergency contacts.

The risk of loss of PII or unauthorized access is low. Risks have been mitigated by implementing technical controls. Users logon to MIS by accessing their workstations with an EDUCATE-issued account followed by a MIS-specific account. MIS can be accessed remotely only with two-factor authentication. The information is stored in a Microsoft SQL database hosted on a server with restrictive access controls.

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.**

SSNs are downloaded from FPPS and used to link the information to the MIS database. No alternative was considered as the SSN is the only unique identifier provided by FPPS.

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.**

The information is used to process personnel actions. The information is analyzed for human capital and budget planning purposes. No specific methods are used to analyze the data except analysis for human capital and budget purposes.

The information is used within the OIG and shared with the Department's Office of Human Resources (OHR). The information is obtained from FPPS Datamart. Some of the information contained within the system consists of employees' grade, step, and salary. This information may be used for considering promotions, opening new positions, and other human capital and budgetary considerations.

7. **Internal Sharing and Disclosure. Which internal DoED organizations will the information being 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.**

PII is shared with the Department's OHR team for personnel related purposes. The risk to privacy is low because the information is only shared with individuals that are authorized to have access to employees' PII. The information is hand carried, sent via interoffice mail, or fax. OHR is notified before fax messages are sent.

8. **<u>External Sharing and Disclosure</u>. 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.**

OIG does not share the information with external entities.

9. **<u>Notice</u>. 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?**

OIG does not collect the information from employees. Employees provide their information (e.g., name, address, date of birth, etc.) directly to the Department's OHR team during onboarding orientation or when changes occur.

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

MIS does not have a web interface. A banner on the log-in window informs users that the system is intended for official government business by authorized personnel and about the consequences of unauthorized access.

11. <u>Security.</u> 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?

Physical and logical controls for MIS are provided by EDUCATE. Access to the system is protected by firewalls, host-based Intrusion Detection System/Intrusion Protection System (IDS/IPS), and antivirus software. MIS is only accessible within the OIG LAN and to OIG employees and contractors with a need to know. Windows and database security logs are reviewed daily. The logs include information about unauthorized logon attempts such as user accounts and the source (ip address) of the attempt.

MIS complies with FISMA and obtained the Authority to Operate (ATO) on 12/5/2012. The MIS application does not interface with other internal or external system.

12. **<u>Privacy Act System of Records.</u> Is the information within the system retrieved by personal identifier? 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?**

The information within the system is retrieved by personal identifier and is covered by OPM/GOVT-1, General Personnel Records, 77 FR 79694 (December 11, 2012).http://dpcld.defense.gov/Privacy/SORNsIndex/DODwideSORNArticleView/tabid/6797/Article/570733/opmgovt-1.aspx

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:

Yes – the Schedule Locator No: ED 066

The NARA Disposition Authority: N1-441-10-1