Privacy Impact Assessment

For: Education Investigative Tracking System (EDITS)

Date: April 10, 2013

Point of Contact: Hui Yang

System Owner: Wanda A. Scott

Author: William Hamel

Office of Inspector General

U.S. Department of Education

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

   The U.S. Department of Education (ED) Office of Inspector General (OIG) Investigations Tracking System (EDITS) is a web-based system that tracks leads, investigations, and complaints that Special Agents and the Hotline Staff, respectively, use for case management and program referral capabilities. The system is designed to facilitate criminal, civil, and administrative investigations of fraud, waste, and abuse in programs administered by the Department of Education. EDITS contains numerous security measures to ensure protection of privacy including grand jury documents and other sensitive information, which is critical to the successful prosecution of violators. Data is manually entered into the EDITS system by the Special Agents from source documents, subpoena records, court records, or during investigative efforts. EDITS is designed to generate specified information and management reports, as well as assist in the overall management and collection of data that is required for successful prosecutions. Data output is typically PDF, MS Excel formats, or in the form of hard-copy reports.

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?**

   5 U.S.C. Appendix, Inspector General Act of 1978, as amended.

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

   Elements of personally identifiable information (PII) that are collected and maintained by EDITS are: name, date of birth, alias, and personal identification-such as Social Security number (SSN), passport number, driver's license number, taxpayer identification number, financial account, credit card number, street address, email address, and personal characteristics including but not limited to: photographic image, fingerprints, handwriting, biometric data, etc.

   PII is obtained from various sources. The most common sources for PII are: taxpayers, employees, grantees, sub-grantees, contractors, students, program participants' family members, institutions, or others with knowledge of fraud, waste, or abuse in Government programs.

   In EDITS, PII originates from several sources such as: (1) personal interviews and investigative activities, (2) public website operated by ED OIG to allow public submissions of complaints of fraud, waste, and abuse using an on-line standardized form, (3) telephone call-in, (4) paper form using the U.S. Postal Service, (5) fax, (6) in-person walk in complaint, (7) National Crime Information Center/National Law Enforcement Telecommunication Service (NCIC/NLETS) databases, and (8) National Student Loan Data System (NSLDS) or other ED student aid systems.

   PII collected during the course of the investigation may be referred to other units within ED. These referrals generally involve complaints being handled through the OIG Hotline where the complainant expressly requests assistance with his or her specific issue. PII is sometimes cross-referenced with information in NSLDS and other internal systems in ED to ensure continuity as well as prevent fraud, waste, and abuse in the administration of programs.

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 any**

type of data collected, discuss the privacy risks (internally and/or externally) identified and how they were mitigated.

PII is obtained to conduct investigations of a criminal, civil or administrative nature involving ED programs and operations. OIG Special Agents rely on PII to accurately identify witnesses, victims, and subjects throughout the investigative process. Information collected and maintained in EDITS is critical to the successful completion of the investigation concerning complaints of fraud, waste, or abuse of Federal funds.

EDITS is an internal system. Access to EDITS is limited to employees who have a need-to-know, direct access to the system, and access to the network where the application resides. This includes OIG Special Agents and internal investigative staff. EDITS is designed so the Personal Identification Verification (PIV) card must be used as a mandatory two-factor authentication that regulates access to the application database. Once the PIV card is authenticated through the use of a Personal Identification Number (PIN), the EDITS user must enter a user account name and password that determines the level of access to EDITS and its database. EDITS requires users to change their passwords every 90 days. Also, by mandating the use of the PIV card to authenticate users, only ED authorized equipment (laptop or desktop) can be used to access EDITS.

Risk has been mitigated by implementing ED policies such as:(1) mandatory use of ED issued PIV, (2) using an ED-issued laptop or desktop with a PIV card reader (3) limiting access to EDITS database to those individuals with established EDITS accounts, and (4) sending notification of improper login attempts to the system administrator each time an unauthorized user tries to access EDITS without proper credentials. Reliance on the PIV card and other user identification factors prevents loss and unauthorized access to PII by providing: user identification, identifying changes made by users, identifying possible sources of unauthorized disclosure, identifying and tracking unauthorized access attempts from non-government issued computers, and other misuse.

5. **Social Security Number (SSN). 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.**

Social Security Numbers (SSNs) are obtained as a way of ensuring the identity of an individual during the course of investigations. Special Agents obtain SSNs of all persons who are subjects of investigations to ensure identity. This identity is cross checked with NSLDS and other systems to ensure that the subject of the investigation is in fact the same person who may be involved in fraud, waste, and abuse of ED or other Federal program funds. The use of the SSN is one of many ways to positively identify persons involved in potential fraud, waste, and abuse. There is no other feasible alternative than using the SSN since the NSLDS and the Free Application for Federal Student Aid (FAFSA) systems use the individual SSN to disburse funds.

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 intended use of the information in EDITS is for law enforcement purposes to include investigations and criminal prosecutions of fraud, waste, and abuse of Federal funds. EDITS is used to account for, process, and track information gathered during the course of an investigation in order to resolve matters concerning the possible existence of an illegal activity or a violation of Federal law.

Methods used to analyze information include the Special Agent's ability to link events, documents, and/or occurrences together in a logical format for the purpose of showing patterns of behavior and relationships associated with an illegal act. The information is used to construct detailed Reports of Investigation (ROI), compile affidavits, search warrants, arrest warrants, and other investigative instruments. All information from public sources, commercial sources or other governmental agencies is acquired to aid the Special Agent in his or her investigation and duty to fully safeguard ED's interest and administration of federal funds.

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?**

Hotline complaints containing PII are routinely shared with the appropriate ED program offices. For instance, a complaint submitted by a student to the OIG Hotline that alleges an institution improperly disbursed student aid would be shared on a routine basis with the Federal Student Aid (FSA) office since the OIG does not typically investigate matters dealing with a single beneficiary. FSA is the appropriate office to timely assist students toward a positive outcome for alleged concerns. The OIG Hotline is the only unit within the agency responsible for receiving and processing complaints and other inquiries from the public related to fraud, waste, and abuse of federal funds in ED programs. However, the vast majority of the complaints that OIG Hotline receives do not necessarily rise to the level of a criminal, civil, or administrative investigation. Matters that do not warrant OIG investigation are typically forwarded by OIG Hotline to the appropriate program offices for resolution. Information is also shared with ED in written formats, such as an Investigation Program Advisory Reports (IPAR) or other documents, when internal control weaknesses are identified through a criminal, civil, or administrative investigation. In this regard, the information will be shared with the program office that has oversight responsibility for taking appropriate corrective action to eradicate said reported weaknesses.

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 or other type of approved sharing agreement with another agency?

Information in EDITS is typically not shared or disclosed externally other than for law enforcement purposes. In many investigations, the subject violator has committed other violations which may fall under the jurisdiction of other law enforcement agencies. In this regard, the Special Agent will share information with the appropriate agency in order to ensure that noted criminal, civil, or administrative violations or weaknesses are addressed. The information is predominately transferred via paper format. In limited situations, such as with the United States Attorney's Office or emergency cases, OIG may transmit documents electronically using password-protected email. OIG prefers to hand-carry hard copy documents or utilize the United Parcel Service (UPS) to transmit any documents that are shared.

The Department may share information contained in EDITS pursuant to the routine uses listed in the Privacy Act system of records notices (SORNs) for the Investigative Files of the Inspector General (18-10-01) and the Hotline Complaint Files of the Inspector General (18-10-04). Information may be shared with external entities without the consent of the individual if the routine use disclosure is compatible with the purposes for which the record was collected. Specific disclosures may include the following:

- Federal, state, local or foreign agencies or law enforcement or oversight agencies

- Public or private entities when necessary to obtain other information
- Institutions, accrediting agencies, and guaranty agencies
- Litigation and alternative dispute resolution
- Contractors and consultants
- Debarment and suspension
- Department of Justice advice
- Congressional member
- Benefit program
- Collection of debts and overpayments
- Council of Inspectors General for Integrity and Efficiency

9. Notice. Is 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?

The Secretary has by regulations exempted the Investigative Files of the Inspector General and the Hotline Complaint Files of the Inspector General from the Privacy Act requirement to give notice to individuals asked to provide information to the Department. (34 C.F.R. § 5b.11(6))

Notwithstanding this exemption, with respect to hotline complaints, the Department provides information about the Privacy Act to complainants via an online form. If the hotline complainant wishes to remain anonymous, the subject complaint can be submitted without the inclusion of any PII.

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

http://www2.ed.gov/about/offices/list/oig/hotline.html

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 C&A been completed? Is the system compliant with any federal security requirements?

Policy and procedure safeguards are used. For example, all Government employees and contractors must have an EDUCATE account prior to receiving access to EDITS. EDITS system user access is granted based on a need-to-know basis and the least allowable privilege needed to perform required duties. All information within EDITS is controlled through network controls, user permissions, user authentication, and database access control. EDUCATE employs firewalls, host-based and network-based Intrusion Detection/Prevention Systems (IDS/IPS), and antivirus software that notify security officers and key EDUCATE administrators of any incidents. EDITS relies on EDUCATE and the General Support Systems (GSS) to monitor physical access to the information system and to respond to physical security incidents. The OIG servers that host EDITS are housed in segregated OIG racks. Access is controlled 100 percent with the racks requiring badge access. An email alert capability has also been implemented. The data centers where the EDITS severs are housed require photo-identification and access permissions from management to enter the buildings. The critical servers and routers are housed in secure rooms that are accessible only to authorized and badged personnel with keycard entry.

EDITS is operational, has an Authority to Operate (ATO) effective August 7, 2009, and is compliant with Federal Information Security Management Act (FISMA) and ED security policies. The system

is currently undergoing modernization and it is being prepared for recertification due to major changes.

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), OIG has already published SORNs covering the systems contained in EDITS. SORNs covering the Investigative Files (18-10-01) are located at 75 FR 36374 (June 25, 2010), 75 FR 33608 (June 14, 2010), and 68 FR 38154 (June 26, 2003). SORNs covering the Hotline Complaint Files (18-10-04) are located at 75 FR 39669 (July 12, 2010) and 64 FR 30157 (June 4, 1999).

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.**

The record schedule number is 218.