Privacy Impact Assessment

For

OIG Case Management System (CMS)

Date:

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

System Owner: Aaron R. Jordan
aaron.jordan@ed.gov

Author: Mark A. Smith
mark.a.smith@ed.gov

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. 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 U.S. Department of Education (ED) Office of Inspector General (OIG) Case Management System (CMS) is an upgrade to the current Education Investigations Tracking System (EDITS), The CMS is a web-based system that tracks complaints, preliminary inquiries, and investigations that OIG Staff 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. The CMS 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 CMS system by the Special Agents from source documents, subpoena records, or during investigative efforts. Data can also be entered into the CMS by the public by entering their report of fraud, waste, or abuse into the Hotline website. The CMS is designed to generate statutorily required information and management reports, as well as assisting in the overall management and collection of data that is required for successful prosecutions. Data output is typically PDF, Microsoft Excel, or text formats.

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 § 6(a)(7), 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 the CMS 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, employees, grantees, sub-grantees, contractors, students, program participants' family members, institutions, or others with knowledge of fraud, waste, or abuse in Government programs.

   In the CMS, PII originates from several sources such as: (1) personal interviews and investigative activities, (2) the Hotline website that enables public submissions of complaints of fraud, waste, and abuse using an on-line standardized form, (3) telephone call-in, (4) paper form through mail or delivery 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 a specific issue. PII is sometimes cross-referenced with information in NSLDS and other internal system in ED to ensure continuity as well as preventing 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 the CMS is critical to the successful completion of investigations concerning complaints of fraud, waste, or abuse of Federal funds.

The risks associated with data collected have been mitigated by the following: The CMS is an internal OIG system that has the appropriate NIST 800-53 Rev 4 controls implemented and has received authority to operate after a thorough assessment of the risk. Security of the system is maintained through continuous monitoring as outlined in NIST 800-13. Access to the CMS is limited to employees who have a need-to-know. This includes OIG Special Agents and internal investigative staff and management. Access to the CMS is limited to user systems connected to the ED network and requires the user to have a valid HSPD-12 Personal Identification Verification (PIV) card and an active CMS account. The requirement to use the PIV card provides for mandatory two-factor authentication to validate the identity of the user. To use the PIV card, the individual must physically possess the PIV card and know the assigned Personal Identification Number (PIN). To gain access to the CMS, the user must also have a valid account, and this account determines the access level the individual has to information within the system. The system also has detailed logging to track successful and unsuccessful login attempts, as well as the activity of users who successfully logged into the system. Additionally, only one session is permitted per user, and all accounts are automatically logged out after 30 minutes of inactivity.

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. 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 an investigation. Special Agents obtain SSNs of all

individuals 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 the CMS is for law enforcement purposes to include the investigation and criminal prosecution of fraud, waste, and abuse of Federal funds. The CMS is used to account for processes and tracks 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 on a need to know basis. 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 investigations are typically forwarded by OIG Hotline to the appropriate program offices for resolution. Information is also shared with ED in written formats, such as a Management Information Report 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 the CMS 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 or other ED approved method for transmitting PII. OIG prefers to hand - carry hard copy documents or utilize the signature required, overnight mail to transmit any documents that are shared.

   The Department may share information contained in the CMS 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 consistent 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 consultant
   - 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.ll(6))

Notwithstanding this exemption, with respect to hotline complaints, the Department provides information about the Privacy Act to complainants on the online hotline complaint form. If the hotline complainant wishes to remain anonymous, the 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.*

https://www2.ed.gov/about/offices/list/oig/hotline.html (current)

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?*

The appropriate NIST 800-53 Rev 4 controls are implemented in the CMS, it has undergone an assessment of risk and received an authority to operate, and continuous monitoring is used to ensure continued technical protections. This includes, but is not limited to, two-factor authentication, encryption of data at rest, and access controls based on user profile. Access to the system can only be achieved from a computer connected to the ED network, and the software and operating system has extensive logging. The infrastructure that hosts the CMS employs firewalls, intrusion detection/prevention systems, anti-virus software, and the system is routinely scanned for vulnerabilities.

Policy and procedure safeguards are also used. For example, all Government employees and contractors must possess at least a 5c public trust clearance and an HSPD-12 PIV card prior to being granted access to CMS. To obtain access, an account must be created within the CMS and appropriate profile will be created to grant access to data based on a need-to-know basis and the least allowable privilege needed to perform required duties.

12. Privacy Act System of Records. *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?

In accordance with 5 U.S.C. § 552a(e)(4) and (l l), OIG has already published SORNs covering the systems contained in the CMS. 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 (18-1 0-04) 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.