Privacy Impact Assessment
For the

Data Analytic System (ODAS)

Date
April 2, 2012

Contact Point
System Owner: Office of the Inspector General
Author: Shelley Shepherd
OIG

U.S. Department of Education

1. **System Information. Describe the system -** The Office of Inspector General Data Analytic System (ODAS) contains personally identifiable information from a variety of individuals who have applied for and/or received grants, contracts, loans, and salary from the U.S. Department of Education (Department). Such individuals include: employees of the Department, consultants, contractors, grantees, advisory committee members, and others who receive funds from the Department for performing services; students applying for Federal student financial assistance; Pell Grant recipients; borrowers of William D. Ford Federal Direct Loans, Federal Family Education loans, Federal Insured Student loans and Federal Perkins loans; owners, board members, officials, and authorized agents of postsecondary institutions; and individuals applying for a Department personal identification number.

Contained within the ODAS system is a collection of analytical modules categorized as the Office of Inspector General Data Analytic System - Decision Support System (ODAS-DSS) that are developed and maintained within the SAS 'Enterprise Business Intelligence (BI) Server' system. This development strategy eliminates the need for constant, ongoing integration of various software application technologies by providing one consistent, fully integrated analytical software platform. The developed ODAS-DSS application modules such as the Metadata Lookup System, Student Lookup System and School Summary System contains useful data search mechanisms that provide both informational and proactive data analytical capabilities to identify patterns of fraud and areas of risk within the Department and Federal Student Aid (FSA) systems.

2. Legal Authority

5 U.S.C. Appendix § 6(a) (The Inspector General Act) authorizes the Inspector General to have access to all records, reports, audits, reviews, documents papers, recommendations, or other material available to the applicable establishment which relate to programs and operations with respect to which that Inspector General has responsibilities under the Act.

3. Characterization of the Information

ODAS maintains names, social security numbers, dates of birth, addresses, phone numbers, email addresses, and bank account numbers of students, Department grantees, contractors, consultants, advisory committee members and other individuals receiving funds from the Department. ODAS extracts records from the following Department systems:

- Education's Central Automated Processing System (EDCAPS) (18-03-02)
- Federal Student Aid Application Files (18-11-01);

- Recipient Financial Management System (the Department soon expects to amend this system and rename it as the Common Origination and Disbursement System) (COD) (18-11-02)
- National Student Loan Data System (NSLDS)(18-11-06)
- Student Financial Assistance Collection Files (18-11-07)
- Postsecondary Educational Participants System (PEPS) (System Number 18-11-09)
- The Department of Education (ED) PIN (Personal Identification Number) (18-11-12)
- Student Authentication Network Audit File (18-11-13)

4. <u>Why is this information being collected?</u>

This information is being collected so that the Department will have access to a single repository of data for purposes of conducting data modeling, investigative and audit assistance, and predictive analytics.

5. <u>Social Security Numbers</u> – 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.

ODAS does not collect any data directly from any individuals, but stores Personally Identifiable Information (PII) data as it is received from other Department and contractor-managed systems as outlined in paragraph 3.

The Department may disclose information contained in ODAS under the routine uses listed in the pertinent system of records notice without the consent of the individual if the disclosure is compatible with the purposes for which the record was collected. These disclosures are 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) Law Enforcement Disclosure
(2) Disclosure to Public or Private Entity to Obtain Relevant Information
(3) Employment, Benefit, and Contracting Disclosure
(4) Higher Education Act Disclosure
(5) Litigation and Alternative Dispute Resolution (ADR) Disclosure
(6) Contractor and Consultant Disclosure
(7) Debarment and Suspension Disclosure
(8) Disclosure to the Department of Justice
(9) Congressional Member Disclosure
(10) Benefit Program Disclosure
(11) Debt Collection Disclosure
(12) Council of Inspectors General for Integrity and Efficiency Disclosure
(13) Qualitative Assessment Review Disclosure
(14) Disclosure in the Course of Responding to a Breach of Data

6. <u>Uses of the Information</u>. 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 this system will be used to identify fraud and systemic control issues, and to improve methods of data analysis and annual audit planning. Information in ODAS will be used for data modeling using statistical and mathematical techniques, in order to identify emerging risk and predict anomalies indicating fraudulent activity involving Department funds.

Under the Inspector General Act of 1978, as amended, 5 U.S.C. Appendix, Inspectors General, including OIG, are responsible for conducting, supervising, and coordinating audits and investigations, relating to programs and operations of the Federal agency for which their office is established. Information in this system will be used in support of audits, investigations and inspections consistent with the OIG's statutory duty.

7. <u>Internal Sharing and Disclosure</u>. Which internal DoED 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.

ODAS extracts data from the Department systems listed in paragraph 3. ODAS information will be shared with Risk Management Services for purposes of assessing risk of potential grantees. ODAS information will also be shared with Federal Student Aid for purposes of highlighting potential fraud that may have been committed by students misusing Title IV funds.

Privacy risks of internal unauthorized disclosure of PII are mitigated by limiting access to ODAS. This system of records limits internal access to data to Department staff on a need-to-know basis and controls individual users' ability to access records within the system. All authorized users of this system are given a unique user identification and are required to establish a complex password that must be changed every 90 days. An automated audit trail documents user activity of each person and device having access to ODAS.

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

The Department may share information from ODAS with external entities pursuant to the routine uses listed in the System of Record notice for ODAS. Information may be shared with other 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.

Privacy risks of external unauthorized disclosure of PII are mitigated by limiting access to ODAS. All authorized users of this system are given a unique user identification and are required to establish a complex password that must be changed every 90 days. An automated audit trail documents user activity of each person and device having access to ODAS.

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?

ODAS does not collect any PII directly from individuals, and therefore 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. A Privacy Act system of records notice covers ODAS and explains the information collected and the entities with which that information may be shared. In addition, there are System of Records notices covering each Department system from which information is obtained and included in ODAS.

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

ODAS is not a publicly accessible system, and is accessible only by authorized internal and external users. Office of Management and Budget memorandum M-03-22, Attachment A, Section III(C)(b), dated September 26, 2003, excludes "agency intranet websites that are accessible only by authorized government users (employees, contractors, consultants, fellows, grantees)" from the requirement to have a posted privacy policy. Accordingly, ODAS is exempt from the requirement to have a privacy notice posted on its website.

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?

The information is secured in accordance with OMB M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003, the E-Government Act, Section 208, Attachment A, and NIST 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*, December 2006.

A. All information stored in this system is secured by utilizing database security technology and is resistant to tampering and circumvention by unauthorized users. Access to data by all authorized users will be monitored using both automated and manual controls. The information is accessed by Department staff on a "need-to-know" basis and intended systems usage basis.

B. ODAS is developed and maintained by the OIG and is housed within a secure and controlled facility. Access to the computer lab is by authorized OIG personnel only. The general public does not have access to ODAS.

C. Interfacing systems from which data will be extracted and maintained are listed under paragraph 1. Individual certification and accreditation packages are required for each of the interfacing systems.

D. System administrators provide comparable security controls to protect the system and the information contained therein.

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 published a System of Records Notice (SORN) for ODAS in the Federal Register. The SORN may be located at 73 FR 61406-61412 (October 16, 2008). The system number is 18-10-02. OIG has submitted an updated Notice of an Altered SORN that is currently being processed for publishing in the Federal Register. This PIA is consistent with the recently submitted Notice of an Altered SORN.

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:

Records in ODAS are retained in accordance to the Department of Education’s schedule ED 122.a. The records will be destroyed/deleted when the Department determines that they are no longer needed for administrative, legal, audit, or other operational purposes.