Privacy Impact Assessment (PIA)

for the

Office of Inspector General Data Analytics System (ODAS)

July 27, 2023

For PIA Certification Updates Only: This PIA was reviewed on **Enter date** by **Name of reviewer** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Nantiepe Kolani/Information System Security Officer
Contact Email: Nantiepe.Kolani@ed.gov

System Owner

Name/Title: Kevin Young/Information System Owner
Principal Office: Office of Inspector General

Please submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov

*Please complete this **Privacy Impact Assessment (PIA)** on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document.*
If a question does not apply to your system, please answer with N/A.

1. Introduction

1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

The Office of Inspector General (OIG) Data Analytics System (ODAS) is an OIG data warehouse system with a web-based front-end application that provides data analytical capabilities to the OIG. ODAS is housed in the Information Technology Audits and Computer Crime Investigations (ITACCI) lab and is connected to the ITACCINet network. The OIG uses ODAS to assist auditors and investigators in identifying fraud, waste, and abuse in U.S. Department of Education (Department) programs. ODAS includes standardized reports that utilize Oracle Business Intelligence (BI) Publisher to assist auditors and investigators to easily and readily identify relevant information related to their audit and investigative efforts. ODAS developers utilize in-depth SQL query capabilities when the standardized Oracle BI Publisher reports are not sufficient for the stated OIG purposes.

ODAS contains personally identifiable information (PII) from a variety of individuals who have applied for and/or received grants, contracts, loans, and/or salaries from the 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, Federally Insured Student loans and Federal Perkins loans; owners, board members, officials, and authorized agents of postsecondary institutions; and individuals applying for a Department Federal Student Aid (FSA) ID.

ODAS receives information from several Department systems, including the Grants Management System (G5), National Student Loan Data System (NSLDS), Common Origination and Disbursement (COD), Digital Customer Care (DCC), Postsecondary Education Participant System (PEPS), Education's Central Automated Processing System (EDCAPS), Central Processing System (CPS), and Person Authentication Service (PAS). ODAS also receives publicly available data (single audit reports conducted by other Federal agencies) from the Federal Audit Clearinghouse. No information is received directly from individuals. The PII collected by ODAS relates to various Department loan and grant programs, enabling OIG to verify identities of borrowers or grantees and take appropriate action (e.g., referring

individuals to Federal, State, or local law enforcement) if ODAS identifies loans or grants that may be the target of fraud, waste, or abuse.

The ODAS application includes modules such as the Purchase Card module, Oracle BI Publisher reports, FSA student information, and FSA school summary information. The Purchase Card module is used to determine if there are any risk-based activities occurring with Department purchase card transactions. Oracle BI Publisher provides a repository of reports that have been created as a result of auditors and investigators requesting similar information from various entities. Examples of this include reports of information gathered from the G5 and single audit reports gathered from the Federal Audit Clearinghouse. ODAS summarizes the information obtained from NSLDS to provide more easily digestible data for OIG auditors and investigators.

1.2. Describe the purpose for which the personally identifiable information (PII)[1] is collected, used, maintained or shared.

ODAS contains PII from a variety of Department systems (e.g., NSLDS, DCC, COD, PEPS, EDCAPS, PAS, G5) and the publicly available Federal Audit Clearinghouse. PII is collected, used, and maintained to assist investigators in conducting criminal and civil investigations and to assist auditors in performing audits for the overall purpose of detecting and preventing fraud, waste, and abuse in Department programs.

Specifically, PII in ODAS is connected to various loan and grant programs that the Department administers. Maintaining the PII is necessary to enable OIG to verify the identities of borrowers or recipients and to take appropriate action (e.g., to make referrals of individuals to Federal, State, or local law enforcement partners or to the appropriate program offices) if loans or grants are identified as potentially being the targets of fraud, waste, or abuse.

1.3. Is this a new system, or one that is currently in operation?

Currently Operating System

1.4. Is this PIA new, or is it updating a previous version?

Updated PIA

The PIA is being updated as part of the required biennial review.

[1] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Circular A-130, page 33

1.5. Is the system operated by the agency or by a contractor?

Agency

1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

☑ N/A

Click here to select.

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, please contact your program attorney.

2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

The Inspector General Act of 1978, as amended (92 Stat. 1101) (the Act). 5 U.S.C. App. § 4 of the Act identifies the responsibilities of the Office of Inspector General which include, among others, providing policy direction for and conducting, supervising, and coordinating audits and investigations relating to the programs and operations of the Department; reviewing existing and proposed legislation relating to programs and operations of the Department; recommending policies for, and conducting, supervising, or coordinating other activities carried out or financed by the Department for the purpose of promoting economy and efficiency in the administration of, or preventing and detecting fraud and abuse in, the Department's programs and operations.

In carrying out these responsibilities, 5 U.S.C. App. § 6(a) of the Act authorizes the Inspector General to have timely access to all records, reports, audits, reviews, documents, papers, recommendations, or other material available to the Department which relate to the programs and operations with respect to which the Inspector General has responsibilities under the Act.

SORN

2.2. Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification?

Yes

Information is retrieved by name or other personal or other institutional identifiers.

2.2.1. If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☐ N/A

The ODAS SORN, entitled the "Office of Inspector General Data Analytics System" (18-10-02), 77 FR 28366, was published in the Federal Register on May 14, 2012.

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

☑ N/A

Records Management
If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov

2.3. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

Since ODAS is used by the OIG for audits and investigations, the data used for those would fall under:

Item V1.D.1: Non-major Audit and Inspection Case Files Disposition Authority Number: DAA-0441-2021-0001-0004
Described as: Files developed during formally approved audits conducted in accordance with the Government Accountability Office's Government Auditing Standards. These records provide the central source of information on work conducted by OIG staff or staff under contract for the OIG for the following:

- Internal audits relating to the programs, operations, and activities of the Department of Education

[2] A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. https://connected.ed.gov/om/Documents/SORN-Process.pdf

- External audits relating to entities doing business with the Department of Education. Entities generally include, but are not limited to, contractors, grantees, lenders, guaranty agencies, state education agencies, local education agencies, schools, and other third parties having an interest in Department programs, operations, and activities
- Also includes files developed during formally approved alternative projects performed in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation. These records provide the central source of information on work conducted by OIG staff or staff under contract for the OIG generally pertaining to, but not limited to, alert memoranda, management information reports, and inspection reports. These projects and files may relate to the programs, operations, and activities of the Department of Education or entities doing business with the Department of Education. Inspections are efficient and independent assessments used to provide Department decision makers with a means to analyze programs quickly and to evaluate operational efficiency, effectiveness, and vulnerability. This work includes special reviews of sensitive issues that arise suddenly and congressional requests for studies that require immediate attention. Inspections are conducted for the purposes of providing timely information to managers for decision-making; monitoring compliance; measuring performance; assessing efficiency and effectiveness; making value-added recommendation for improvements to programs, policies, or procedures; and sharing best practices. The Office of Investigations (IS) and Office of Audits (AS) include a field in the OIG Case Management System to indicate if a case is major (has received national news attention or fulfills the other stated criteria). The field is completed when the investigation or audit is closed; management officials as well as the case agent or auditor in charge are involved in the determination; and the determination is used when AS and IS prepare records for archiving annually.

  Final Disposition: Temporary
  This item is media neutral. [so fully applicable to a system such as ODAS]
  Cutoff Instruction: Cutoff at end of fiscal year in which audit or alternative projects are closed (final action is completed) by the Department.
  Retention Period: Destroy 15 year(s) after cutoff.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes

3. Characterization and Use of Information

Collection

3.1. List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

From aid recipients, parents of dependent aid recipients, spouses of aid recipients (if applicable), endorsers, co-signers, third-party preparers and applicants for loans: name, Social Security number (SSN), date of birth, address, phone number, email address, driver's license number and State, citizenship status, dependency status, employer identification number, affiliation, veteran status, marital status, gender, current income, asset information, expected family contribution, family size, highest level of education completed (for parents and spouses), and loan and grant information (including amount, disbursements, dates of disbursements, balances, repayment plans, loan status, collections, claims, deferments, forbearances, refunds, cancellations, overpayment amounts, and date of default).

From Federal employees accessing the system: username.

From Federal employees involved in purchase card transactions: name, work email address, work address, work phone number, and purchase card number.

From primary contacts of vendors that have contracts or purchase card transactions with the Department: name, work phone number, work email address, and work address.

From grantees: name, phone number, email address, address, bank account number, and bank routing number.

From grant applicants: name, phone number, email address, and address.

All information in PEPS is received by ODAS. Information in PEPS includes:

- Sole proprietorship schools: owner name, SSN, email address, username, and phone number.
- Non-sole proprietorship schools (non-profit and for profit): title (e.g., President), name, work email, username, and work phone number.

3.2. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

OIG maintains only the minimum information necessary for its program oversight purposes. For example, contact information is sometimes needed to communicate with the recipients. Additional information, such as SSNs, is needed to track borrowers throughout the student aid lifecycle and to identify the student. No information is collected that is not required to achieve this purpose. Without the necessary information, OIG would not be able to conduct proper audits and/or investigations for identifying fraud, waste, and abuse in Department programs.

3.3. What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

ODAS does not collect data directly from individuals.

PII is received from the following Department systems:

- Grants Management System (G5)
- Central Automated Processing System (EDCAPS)
- Common Origination and Disbursement System (COD)
- National Student Loan Data System (NSLDS)
- Person Authentication Service (PAS)
- Digital and Customer Care (DCC)
- Postsecondary Education Participants System (PEPS)

PII and/or information is also received from the following external entities:

- U.S. Census Bureau - Federal Audit Clearinghouse (audits conducted by other Federal agencies)
- General Services Administration - Department Purchase Card Data extracts provided under the General Services Administration Charge Card Master Contract

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

ODAS securely collects files containing PII from its data sources through file database extracts and compiles the data into ODAS tables for analysis. This process is managed through Memorandums of Understanding (MOU) with the Office of Federal Student Aid and with the Office of the Chief Information Officer. ODAS does not have any direct connections to any of its data sources listed in Question 3.3. For

the publicly available Federal Audit Clearinghouse data, we utilize the public data extract available at the Federal Audit Clearinghouse website.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[3] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

When ODAS receives data from the various systems listed in Question 3.3, it performs data reliability and validity checks to assure all of the data are received and processed accurately. A few different methods are used to verify the integrity of the data file received, depending on how the file was transferred. This would be done automatically by the application used to package and/or transmit the data file or it would be performed manually from details provided by the sender. ODAS uses record counts provided by the data source to verify the data within the file once extracted. The ODAS import scripts and database structure have the expected data field parameters from the source provided data dictionary and they will produce an error when an unexpected value is encountered. The data are imported into the database as read-only and the database application continuously monitors for data changes through logging and auditing.

Use

3.6. Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

This information is being collected for OIG to have access to a single repository of data for purposes of assisting in the conducting of investigative and audit assistance. ODAS obtains data from various Department systems, as well as the U.S. Census Bureau and the General Services Administration. The PII is required to review and analyze the data to prevent and detect fraud, waste, and abuse in the programs and operations of the Department.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

3.7.1. If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?

[3] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

☑ N/A

Social Security Numbers

It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

3.8. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

Yes

3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

☐ N/A

SSNs are maintained because ODAS utilizes data from multiple systems that rely on the SSN to identify applicants, borrowers, and other individuals. SSNs are used in the source systems, listed in question 3.3, as they are the only reliable method of tracking applicant, borrower, other individual, and employee information across multiple internal and external sources (i.e., servicers) to the Department. ODAS collects SSNs from Department systems to conduct audits and investigations into fraud, waste, and abuse in Department programs and operations.

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☐ N/A

While alternatives were considered, the SSN are required to uniquely identify applicants, borrowers, parents of borrowers, spouses of borrowers, and other individuals. Source systems, listed in question 3.3, require the ability to match applicant and borrower records, as well as records on other individuals, with those maintained in Department systems as well as those outside the Department, such as servicer systems. The SSN is the only universal unique identifier that is used to match records across these systems. Since SSNs are used by these source systems as the only universal unique identifier, ODAS has no alternative to collecting SSNs when obtaining information from these systems.

4. Notice

4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

ODAS does not collect any PII directly from individuals and therefore does not provide a privacy notice to individuals about whom it collects PII. Individuals are provided notice by the source systems from which ODAS retrieves information. Please review the PIAs for the source systems listed in Question 3.3 for further information. The Department PIA website is located at https://www2.ed.gov/notices/pia/index.html.

Additionally, notice is provided though the publishing of the System of Records Notice referenced in Question 2.2.

4.2. Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

☑ N/A

4.3. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

Individuals do not have the ability to consent to additional uses, decline to provide information, or opt out of their information being maintained in ODAS. Opportunities to decline to provide PII or opt out are at the initial point of collection.

4.4. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

☑ N/A

5. Information Sharing and Disclosures

Internal

5.1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

Yes

5.2. What PII will be shared and with whom?

☐ N/A

The OIG shares analytical results containing individuals' names, SSNs, dates of birth, addresses, and any other relevant information (e.g., in the case of persons involved in fraud rings, schools they attended, financial aid history, amounts of loans disbursed to them) with FSA, if analyses indicate those individuals may be engaged in fraud or abuse.

5.3. What is the purpose for sharing the specified PII with the specified internal organizations?

☐ N/A

OIG shares PII that has been analyzed and processed within ODAS related to individuals for whom evidence suggests the possibility of fraudulent activity.

External

5.4. Will the PII contained in the system be shared with external entities (e.g. another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.

Yes

5.5. What PII will be shared and with whom? List programmatic disclosures only.[4] **Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose**.

☐ N/A

OIG may share information from ODAS with external entities pursuant to the routine uses listed in the SORN 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. Please refer to the SORN listed in question 2.2.1 for a comprehensive list of routine uses.

5.6. What is the purpose for sharing the PII with the specified external entities?

☐ N/A

[4] If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

OIG may share information from ODAS with external entities pursuant to the routine uses listed in SORN for ODAS. These are primarily for determining if fraudulent activities are occurring.

5.7. Is the sharing with the external entities authorized?

☐ N/A

Yes

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☐ N/A

Yes

5.9. How is the PII shared with the external entity (e.g. email, computer match, encrypted line, etc.)?

☐ N/A

Information is shared in a secure fashion normally through various secure encrypted file sharing applications depending on the security requirements of the Department and the recipients listed above.

5.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

☐ N/A

Yes

5.11. Does the project place limitation on re-disclosure?

☐ N/A

Yes

6. Redress

6.1. What are the procedures that allow individuals to access their own information?

This system is exempt from the records access provisions in 5 U.S.C. 552a(d)(1) and record access procedures in 5 U.S.C. 552a(e)(4)(H) pursuant to 5 U.S.C. 552a(k)(2)

and 34 CFR 5b.11(c)(1). Please review the PIAs for source systems for further information about accessing and correcting information in those systems.

6.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

This system is exempt from the contesting record provisions in 5 U.S.C. 552a(d)(2-4) and contesting record procedures in 5 U.S.C. 552a(e)(4)(H) pursuant to 5 U.S.C. 552a(k)(2) and 34 CFR 5b.11(c)(1). Please review the PIAs for source systems for further information about accessing and correcting information in those systems.

6.3. How does the project notify individuals about the procedures for correcting their information?

This system is exempt from the notification procedures in 5 U.S.C. 552a(e)(4)(G) pursuant to 5 U.S.C. 552a(k)(2) and 34 CFR 5b.11(c)(1). Please review the PIAs for source systems for further information about procedures to access and correct information in those systems.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

7.2. Is an Authorization to Operate (ATO) required?

Yes

7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

☐ N/A

Moderate

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

ODAS is maintained on secure computer servers located in one or more secure

Department network server facilities. Access to ODAS is limited to authorized Department personnel. Multifactor authentication is required to access ODAS. Access can only be gained by using both the Department's internal network and OIG's internal network, ITACCINet. ODAS is developed and maintained by the OIG and is housed within a secure and controlled facility. Access to the computer lab is limited to authorized OIG personnel only. The public does not have access to ODAS and is only accessible by Department employees. ODAS data are encrypted in transit and while at rest. Monitoring controls are in place to determine if there is unauthorized access. Monitoring of unusual downloading of the data is also in place.

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and Office of Management and Budget (OMB) policy, ODAS must receive a signed Authorization to Operate (ATO) from a designated Department authorizing official. Security and privacy controls implemented by ODAS are comprised of a combination of administrative, physical, and technical controls.

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

7.7. Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

The ODAS security team conducts a yearly self-assessment of selected security controls. All applicable NIST security controls applicable to a moderate system are assessed within a three-year cycle. A yearly report of the results is written and any risks that are identified are noted and tracked for correction. The yearly report is presented to the system owner and authorizing official and any required corrective actions are discussed. Also, the OIG conducts its own periodic independent assessments.

The following tasks are performed to safeguard ODAS information:

- Monthly vulnerability scans performed.

- Quarterly assessments are performed on a quarter of security controls as part of the Ongoing Security Assessment process.
- Annual contingency plan test performed.
- Annual self-assessments conducted and/or annual security assessments performed by the Department Security Authorization Team.
- Annual updates to system security documents.
- Annual mandatory Cybersecurity and Privacy Training for employees and contractors.
- Monthly Continuous Monitoring is in place with vulnerability scans, hardware/software inventories, and configuration management database updates are documented.

8. Auditing and Accountability

8.1. How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

The system owner works with the Department's Privacy Program to complete a PIA and to ensure the PIA is accurate and updated as required. The system owner also completes the Department Risk Management Framework process to secure an ATO. The system owner works with contractors to ensure the system is being used appropriately and in accordance with the practices detailed in this document. In addition, all ODAS users sign a user agreement that indicates the proper use of the data and the consequences of not following the rules of behavior. User accounts are reviewed annually to assure only authorized OIG employees have access.

8.2. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

8.3. What are the privacy risks associated with this system and how are those risks mitigated?

Privacy risks associated with ODAS include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include identity theft, embarrassment, or financial loss. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department. To further mitigate this risk, the following safeguards have been implemented:

- Monthly vulnerability scans
- Annual contingency plan test
- Annual or ongoing security assessments

Risks are also mitigated by updating security patches and updating devices' operating software. Scans are run on the production environment each month in support of the monthly patching cycle. Collecting the minimum PII necessary to achieve the system's purpose also mitigates privacy risks.