Privacy Impact Assessment (PIA)

for the

Office of Inspector General Data Analytics System (ODAS)

November 23, 2020

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: Zachary T Sudiak
Contact Email: Zachary.Sudiak@ed.gov

System Owner

Name/Title: Robert Mancuso, Assistant IG for ITACCI
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 Data Analytic System (ODAS) is a data warehouse system that provides the OIG with data analytical capabilities. ODAS contains a collection of analytical modules that assist auditors and investigators in identifying fraud, waste, and abuse.

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

ODAS contains personally identifiable information from a variety of U.S. Department of Education (ED) systems (e.g., the National Student Loan Data System, the Common Origination and Disbursement System, the Postsecondary Education Participants System) and the publicly available Federal Audit Clearinghouse. PII is collected, used, and maintained in order 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 ED programs.

Specifically, PII in ODAS is connected to various loan and grant programs that ED administers. ODAS maintains PII throughout the life cycle of loans and grants administered under various ED programs. Maintaining the PII is necessary to enable the 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 ODAS analysis identifies loans or grants, at any point in their lifecycles, that may be the target of fraud, waste, or abuse.

[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

1.3. 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

This PIA is being updated in accord with Department policy requiring PIAs be reviewed and updated every two years

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.

5 USC App. § 4 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 ED; reviewing existing and proposed legislation relating to programs and operations of ED; recommending policies for, and conducting, supervising, or coordinating other activities carried out or financed by ED for the purpose of promoting economy and efficiency in the administration of, or preventing and detecting fraud and abuse in, the ED's programs and operations.

In carrying out these responsibilities, 5 U.S.C. App. § 6(a) (Inspector General Act of 1978, as amended) authorizes the Inspector General to have timely access to all records, reports, audits, reviews, documents, papers, recommendations, or other material available to ED 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

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 Office of Inspector General Data Analytics System," 18-10-02, originally published October 16, 2008 (73 FR 61406) and amended May 14, 2012 (77 FR 28366). The complete SORN can be found here: https://www2.ed.gov/notices/sorn/18-10-02-full-publ.pdf

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

Click here to enter text.

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.

ODAS follows the originating component's or organization's records retention schedule for those relevant records and information. So, for example, ODAS follows NSLDS NARA DISPOSITION AUTHORITY: DAA-0441-2017-0004 for the NSLDS data that it receives. We are now developing a comprehensive records retention and disposition schedule for all of the information included in this system of records. Until NARA approves a retention and disposition schedule for those records not covered by other

[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

NARA disposition authority, OIG will not destroy those ODAS records. Records that are provided to Investigative or Audit Services will be retained per OIG NARA DISPOSITION AUTHORITY: N1-441-02-1.

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.

Records in ODAS include:
Direct personal identifiers for borrowers, parents of dependent borrowers and spouses if applicable such as full name, Social Security Number (SSN), date of birth, home/current address, home/work/alternate/mobile telephone numbers, email address, driver's license number and state, citizenship status, dependency status, veteran status, marital status, and gender; income information for borrowers, parents, and spouses if applicable such as current income, asset information, expected family contribution, family size, highest level of schooling completed (for parents and spouses), and pre-and post-screening results that determine a parent's aid eligibility; loan and Grant Information such as amount, disbursements, dates of disbursements, balances, repayment plan, loan status, collections, claims, deferments, forbearances, refunds, cancellations, overpayment amounts, and date of default.

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.

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

ODAS does not collect any data directly from any individuals but maintains Personally Identifiable Information (PII) as it is received from the following Department systems:
• Education's Central Automated Processing System (EDCAPS) (18-04-04)
• Federal Student Aid Application Files (18-11-01)
• Common Origination and Disbursement System) (COD) (18-11-02)
• National Student Loan Data System (NSLDS) (18-11-06)
• The Department of Education (ED) PAS (Person Authentication Service) (18-11-12)
• Student Authentication Network Audit File (18-11-13)
• Data extracts from ED purchase card servicer

ODAS also includes data retrieved from the Federal Audit Clearinghouse.

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 collects the PII from the sources stated above using secure Extract, Transform and Load (ETL) processes. We have Memorandums of Understanding (MOU) with Federal Student Aid and with the Office of the Chief Information Officer for these processes.

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 we receive the data from the various systems listed in section 3.3 above, we perform reliability checks to assure all of the data was received and processed accurately. We also process select address data through other software to assure that it is reliable and accurate. For example, we process the address data through standardization process software to assure we are using the most consistent, reliable data in our internal analytics. If we note anomalies in our data during our analytics process, we review our internal data first to assure that our processes did not cause the anomaly. Then, if our system and processes did not cause the error, we contact the system that provided the data to have them research their data to identify the cause or issue.

Use

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

[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.

This information is being collected so that OIG will have access to a single repository of data for purposes of conducting data modeling, investigative and audit assistance, and predictive analytics. ODAS obtains data from various Department systems, and the PII is required to review and analyze the data in order to prevent and detect fraud 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?

☑ N/A

Click here to enter text.

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 and borrowers.

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

☑ N/A

Alternatives to using SSNs have been considered in the originating systems of records. The alternatives have not been selected because the systems interface with

other systems and all of them rely on SSN to identify students, loans, grants, and over-payments.

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 this notice when information is collected by the Department in the context of each system from which ODAS receives extracts. Additionally, notice is provided though the publishing of the System of Records Notice referenced in Section 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

Click here to enter text.

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 specifically 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?

Yes

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 with Federal Student Aid 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) 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

We share PII that we have obtained from FSA systems that has been analyzed and processed within ODAS where we have evidence to suggest that there is possible fraudulent activity occurring.

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 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. 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

[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.

• Congressional member
• Benefit program
• Collection of debts and overpayments
• Council of the Inspectors General on Integrity and Efficiency.

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

☐ N/A

OIG may share information from ODAS with external entities pursuant to the routine uses listed in SORN for ODAS. These are 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 always shared in a secure fashion normally through a secure encrypted file sharing application.

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?

The ODAS system is investigatory material compiled for law enforcement purposes that is exempt from certain provisions of the Privacy Act including the provisions regarding access to records. See 5 U.S.C. § 552a(k)(2) and 34 C.F.R. § 5b.11(c)(1). Nonetheless, individuals would have records access rights to their records in the system from which their records in ODAS were derived if those systems are systems of records under the Privacy Act.

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

The ODAS system is exempt from Privacy Act record access requirements. However, the individual would have records access rights to their records in the originating system if those systems are systems of records under the Privacy Act.

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

The originating system of records notice listed in question 3.3 and this PIA explains the procedures for correcting customer information.

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 Authority 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?

Only authorized and approved users have access to ODAS. Access is extremely limited and controlled. Multifactor authentication is required to access ODAS. Access can only be gained by using both the ED and ITACCINet internal networks. 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 general public does not have access to ODAS. ODAS data is 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.

Moreover, ODAS has received an Authorization to Operate and has put in place all required controls at the moderate categorization level under NIST standards.

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 National Institute of Standards and Technology 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. The results are reviewed with them and any required corrective actions are discussed. Also, a periodic independent assessment is performed of ODAS. The latest independent assessment was completed in September 2019. Vulnerability scans are conducted weekly on ODAS.

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?

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?

ODAS uses and maintains PII as described above. This PIA details the privacy controls and safeguards implemented for this system. These controls and safeguards work to protect the data from privacy threats and mitigate the risks to the data.

Key risks include unauthorized access to the system and misuse of the PII. In order to further mitigate those risks, the following safeguards have been implemented beyond those described above:

Any system from which ODAS receives data has a memorandum of understanding as to the secure data transfer process and the approved uses of the data.
As mentioned previously in this document, there are very limited users of ODAS data, and all users are approved and sign an agreement as to the proper use of the data. ODAS does not have any public access. All of ODAS access is from internal network connections using multi-factor authentication. The user list is reviewed annually, and users are removed when they leave the organization or change positions. There are controls in place to monitor and review when unusual activity occurs. All of the ODAS data is encrypted when at rest.