Privacy Impact Assessment (PIA)
for the

Maximus Intelligent Virtual Assistant (MIVA)
January 18, 2024

Point of Contact

Contact Person: Adebowale Eniayewun
Title: Information System Security Officer
Email: Adebowale.Eniayewun@ed.gov

System Owner

Name: Shital Shah
Title: System Owner
Principal Office: Federal Student Aid (FSA)

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

*Please complete this **Privacy Impact Assessment (PIA)**, which describes 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, answer with N/A.

- **Please ensure all responses are written in plain language. Write out all acronyms on first use and use acronyms consistently thereafter.**

- **For questions that are identical to those in the Privacy Threshold Analysis (PTA), please review the responses provided in the most recently approved PTA, determine whether the responses remain accurate, and, if so, use the same response in the PIA.**

1. Introduction

1.1. Describe the project or program that uses this information technology (IT) system, including the purpose of the project or program.

Aidvantage (ADVS) is a contractor responsible for servicing Title IV student loans under the Higher Education Act of 1965 (Title IV), as amended, on behalf of Federal Student Aid (FSA) within the U.S. Department of Education (Department). ADVS services borrower accounts from origination through the end of the loan life.

Within the FSA ecosystem, ADVS is one of the core Title IV Additional Servicers (TIVAS) that, along with additional not-for-profit servicers (NFPs), primarily perform direct loan servicing on behalf of FSA for an assigned portfolio of borrowers with non-defaulted student loans. Each FSA servicer maintains its own contact centers for intake of questions from borrowers. These contact centers may use systems that are different from other servicers' contact center systems.

The Maximus Intelligent Virtual Assistant (MIVA), described below, is a core piece of the technology upgrades being made to the ADVS contact center to increase service quality.

1.2. How does the IT system function to support the project or program as described in Question 1.1?

MIVA is a FedRAMP-authorized software-as-a-service (SaaS) system. MIVA is a hosted interactive voice response (HIVR) system that is being used by ADVS to offer automated voice services to aid recipients, cosigners, and/or endorsers calling for contact center assistance with Federal student loans. MIVA contains an automated speech recognition (ASR) engine that facilitates automatic responses to callers, as well as the capability for intervention by an Intent Analyst (IA) when the ASR cannot properly discern a response.

MIVA is a telephony routing system that provides interactive responses to callers. It helps categorize and route calls from individuals contacting ADVS. MIVA utilizes the ASR engine to ascertain the nature of callers' questions and direct them to the appropriate next steps. MIVA requests callers' personally identifiable information (PII) to verify their identities. This information is not stored or recorded within MIVA, which uses an application programming interface (API) to verify caller-provided information by referencing records within the ADVS system boundary.

When the ASR does not understand information received from the aid recipients, cosigners, and/or endorsers of loan applications due to ambiguity, background noise, or other factors, a voice snippet is instantly delivered to a live ADVS agent, the IA. These voice snippets are less than ten seconds in duration on average. The IAs will hear the voice snippet in near real-time and inform the HIVR system of the caller's response or intent, which allows the HIVR to seamlessly continue the call. The IAs never interact directly with the caller. MIVA is configured to deliver utterances in a randomized manner so that IAs are less likely to receive more than one utterance from a single caller. Voice snippets are temporarily stored within MIVA and then transferred to a cloud boundary outside of MIVA.

MIVA solicits PII from borrowers responding to automated call center questions. Verification of callers' identities is required to allow callers to perform self-service functions through MIVA such as obtaining loan balances, making payments, editing contact information, and resetting passwords. Two forms of identification are required for self-service:

- The caller must first provide either their Social Security number (SSN) or their customer identification number (CIN), an identifier assigned by ADVS when an account is created for ADVS.
- The caller must then provide the phone number associated with their account. If the phone number provided does not match the one stored in the account, the caller must provide date of birth (DOB) as an alternate method of identification.
- If the caller does not provide the required information or the information does not match existing records, the caller is transferred to an ADVS agent within the ADVS system boundary.

Call logs are also stored within the ADVS system boundary using a "Call ID" assigned to each call when contact with MIVA is initiated.

1.3. What are the technical elements and/or components of the Information Technology (IT) system? Mark all that apply.

☐ Website	☐ Portal	☒ Application
☐ Database	☐ Server	☐ Other (Specify Below)

If you have been directed to "specify below," describe the type of technical elements and/or component:

1.4. Describe the purpose for which the personally identifiable information (PII)[1] is created, collected, used, processed, stored, maintained, disseminated, or disclosed by the IT system. If there is more than one type of individual from whom PII is collected (e.g., grantees, parents, Federal employees, contractors), specify the purpose for each type of individual.

MIVA requests callers' PII, including SSN, phone number, and DOB, to verify their identities before allowing them to perform self-service functions through MIVA. Additional PII such as mailing address and email address may also be collected through MIVA to facilitate self-service functions such as changing contact information.

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

Contractor

1.6. If the IT system is operated by a contractor, describe the contractor's role in operating the system.

☐ N/A

ADVS hosts the application, processes the phone calls received by the application, and provides the IAs who interpret unclear responses.

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

Yes

☐ N/A

2. Legal Authorities and Other Requirements

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

2.1. What specific legal authorities permit and regulate the collection and use of data by the IT system? Include name and citation of each authority.

[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

The system is authorized by the Higher Education Act of 1965 (20 U.S.C. 28 § 1001 et seq.), as amended, and Executive Order 9397 (November 22, 1943), as amended by Executive Order 13478 (November 18, 2008).

System of Records Notice (SORN)

2.2. Has the Department's Privacy Program determined that the PII maintained by the IT system is or will be maintained as part of a Privacy Act system of records? Refer to the "SORN" item in the "Privacy Program Determination" section of the PTA if unsure.

☒ Yes

☐ No

2.3. If yes, provide the full name(s), number(s), and Federal Register citation of the applicable SORN(s) and/or a statement indicating that a new or modified SORN is being prepared.

The SORN, titled, Common Services for Borrowers (CSB) (18-11-16), 88 FR 48449, was published in the Federal Register on July 27, 2023.

Records Management

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

2.4. Is there an applicable records retention schedule(s) for the information maintained in the IT system? Note: If no records schedule is in place or you are unsure of the applicable records schedule, reach out to your records liaison or the Records Management Office.

☐ Yes, there is/are approved records retention schedule(s) for the information. List the schedule(s):

☒ No, there are currently no approved records retention schedules, but there is a proposed schedule or plan to establish a schedule. Explain:

This system is under review for its revised record retention and subsequent NARA approval. Records will be safeguarded as permanent pending NARA approval.

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

☒ Yes

☐ No

3. Information Collection, Maintenance, Use, and/or Disclosure

Collection

3.1. Select the types of PII that are collected, maintained, used, and/or disclosed by the IT system. **Note:** PII includes any information that is linked or linkable to an individual, including business or contact information, information that is publicly accessible elsewhere, and ordinarily non-sensitive information.

Biographical and Contact Information

☐ Name	☒ Date of Birth	☐ Gender or Sex
☐ City, State, or County of Birth	☐ Country of Birth	☒ Home Address
☒ Personal Phone Number	☐ Work Phone Number	☒ Personal Email Address
☐ Work Email Address	☐ Work Address	☐ Personal Fax Number
☐ Work Fax Number	☐ Digital Signature ☐ Hand Signature	☐ Mother's Maiden Name

Other Demographic Information

☐ Citizenship and/or Alien Registration Number (A-Number)	☐ Military Service	☐ Marital Status, Spouse, and/or Child Information (Specify below)
☐ Educational Background/Records	☐ Group/ Organization Membership	☐ Employment Information
☐ Physical Characteristics or Biometrics (Height, Weight, etc.)	☐ Race/Ethnicity	☐ Religion

Identification Numbers

☒ Social Security Number	☐ Truncated/Partial Social Security Number	☐ Driver's License Number
☐ Passport Number	☐ Employee Identification Number	☐ Professional License Number
☐ Credit/Debit Card Number	☐ Bank/Financial Account Number	☐ Personal Device Identifiers/Serial Numbers
☐ License Plate Number	☐ File/Case ID Number	☐ Federal Student Aid Number
☐ Student ID Number	☒ Student Loan Number	☐ Grant Number
☒ Other ID That Can Be Traced to Individual (Specify below)		

Electronic and Miscellaneous Information

☐ Username/User ID	☐ Password	☐ IP Address
☐ MAC Address	☐ Complaint Information (Specify below)	☐ Medical Information (Specify below)
☐ Location Data	☐ Log Data That Can Be Traced to Individual	☐ Photographs of Individuals
☐ Videos of Individuals	☐ Criminal history	☐ Other (Specify below)

If you have been directed to "specify below," describe the PII: Customer Identification Number (CIN). The CIN is the internal AidVantage account number assigned to aid recipients.

3.2. Select the category of individuals from whom information is collected, maintained, used, or disclosed by the IT system and, if applicable, list what information from Question 3.1 is collected from each. Check all that apply:

☐ Federal Employees

Specify types of information collected from Federal employees:

☐ Federal Contractors

Specify types of information collected from Federal contractors:

☒ General Public (Any individual not employed by the Department).

Specify categories of the general public (e.g., teachers, students, parents, institution representatives, grantees, State and local government employees), and the types of information collected from each:[2]

From aid recipients and their spouses, cosigners, and endorsers of loan applications: DOB, phone number, mailing address, email address, SSN, CIN, and any other information related to loans retrieved from ADVS.

While the system does not require or solicit any PII other than what is listed above, callers may self-disclose additional information during a call.

3.3. What are the sources of PII collected, maintained, used, or disclosed by the IT system (e.g., individual, school, another agency, commercial sources)?

PII is collected from aid recipients, cosigners, and endorsers of loan applications contacting ADVS for assistance regarding student loans. PII collected through MIVA for identity verification is matched against existing records within ADVS. Loan information obtained from ADVS may be communicated to the caller depending on the functions used by a caller during a call.

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

[2] For example:
From students: name, email address, phone number.
From institution representatives: name, email address, username, password.

Aid recipients, cosigners, and endorsers of loan applications orally provide information within MIVA to respond to automated call center questions.

3.5. Privacy law and policy generally requires agencies to collect or maintain only the minimum amount of PII necessary to accomplish an authorized purpose. For each of the PII elements that are indicated in Question 3.1, please describe why the information is necessary.

SSN, CIN, phone number, and DOB are collected to verify callers' identities with information maintained in ADVS. Mailing address and email address can be submitted by callers updating their contact information in ADVS via MIVA.

3.6. Who can access the information maintained in the IT system?

☒ Federal Employees
☒ Federal Contractors
☒ General Public (Any individual not employed by the Department).

NOTE: Aid recipients, cosigners, and/or endorsers can only access information regarding their specific loan within MIVA.

3.7. How is the PII validated or confirmed to ensure the integrity or quality of the information (e.g., form restricting, verifying newly collected information matches previously collected information, account verification, periodically requesting system users verify their own information in the system)?

Information provided by callers is matched with information maintained in the ADVS database. If information provided by callers does not match information maintained in ADVS, callers may not perform self-service activities within MIVA and will be transferred to an ADVS agent.

Information Use for Testing

3.8. Is the PII maintained in the IT system used for internal testing, training, and researching new applications or information systems?

No

3.8.1. If the above answer to question 3.8 is **YES**, are you authorized to use PII when such information is used for internal testing, training, and research?

☑ N/A

Click here to select.

3.8.2. If the above answer to question 3.8 is **YES,** what controls are in place to minimize the privacy risk and protect the data?

☑ 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.

3.9. Does the IT system collect or maintain Social Security numbers (SSNs)?

Yes

3.9.1. If the above answer to question 3.9 is **YES**, cite the authority for collecting or maintaining the SSNs.

☐ N/A

The collection of SSNs of users of this system is authorized by 31 U.S.C. 7701 and Executive Order 9397, as amended by Executive Order 13478 (November 18, 2008).

3.9.2. If the above answer to question 3.10 is **YES**, explain the purpose for the collection/maintenance and how the SSNs are used.

☐ N/A

SSNs are used to verify callers' identities based on matching information provided by the caller with information maintained in ADVS.

3.10.3. If the above answer to question 3.10 is **YES**, specify whether the collection of the SSNs is mandatory or voluntary. What are the consequences for the individual of not providing the SSN, if any?

☐ N/A

SSNs are not required if callers are able to provide their CINs. If callers are unable to provide their CINs, they must provide SSNs. If callers are unable to provide their SSNs or CINs, then MIVA will transfer the caller to an ADVS agent.

3.10.4. If the above answer to question 3.10 is **YES**, specify any alternatives to SSNs that were considered and explain why they were not used.

☐ N/A

While CINs may be used as an alternative to SSNs, many callers do not know their CINs. SSNs are the only other reliable identifier that can be used for identity verification by the system without making the system unusable to many callers.

4. Notice

4.1. How does the IT system provide individuals with a privacy notice about the collection, maintenance, use, and disclosure of PII prior to its collection? For example, does the IT system provide a Privacy Act Statement (if applicable) or other privacy notices provided at the point of collection? If a notice is not provided, explain why not.

If a caller requests information pertaining to privacy while interacting with MIVA, the call will be transferred out of MIVA to a live agent within the ADVS system. The agent will provide information on how to access the ADVS privacy statement to the caller.

4.2. If you, or a partner, maintain a program website that is not hosted on the ed.gov domain and is accessible to the public, does the program website have a webpage privacy policy?

Yes

4.3. Provide a link to the webpage where the privacy notice referenced in Question 4.1 is posted. If there is no publicly accessible link, provide the text of the privacy notice. Do not include security banners, security notices, Paperwork Reduction Act statements, or other notices not specifically related to privacy.

☐ N/A

The ADVS privacy statement can be found at the following URL: https://www.aidvantage.com/privacy-statement.

4.4. What opportunities are available for individuals to consent to uses of their PII, decline to provide PII, or opt out of the project? If these options are not available, state why not.

While providing information to MIVA is voluntary, providing certain PII is required to verify the caller's identity. This information is required for further interactions with the MIVA HIVR and/or an ADVS agent if the call is transferred out of MIVA.

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

Yes

5. Information Sharing and Disclosures

Internal

5.1. Is PII maintained in the IT system shared internally with any other Department IT system(s) and/or principal offices? If the answer is **NO**, skip to Question 5.4.

No

5.2. Which categories of PII from Question 3.1 are shared and with which Department IT system(s) and/or principal offices?

☑ N/A

5.3. What is the purpose for sharing the specified PII with each Department IT system(s) and/or principal office specified in Question 5.2?

☑ N/A

External

5.4. Is PII maintained in the IT system shared with any external entities (e.g., another agency, grantee, school district, the public)? If the answer is **NO**, skip to Question 6.1.

No

5.5. Which categories of PII from Question 3.1 are shared and with whom?

☑ N/A

5.6. What is the purpose for sharing the PII with each external entity specified in Question 5.5?

☑ N/A

5.7. What are the specific authorities that authorize sharing the PII with the external entities specified in Question 5.5?

☑ N/A

5.8. Does the IT system maintain an accounting of any disclosures made to an external entity?

☑ N/A

Click here to select.

5.8.1. If so, is the accounting of disclosures made to external entities available in response to a Privacy Act request?

N/A

5.9. How is the PII shared with the external entity (e.g., encrypted email, transport layer security (TLS) line)? Specify whether the PII is encrypted in transit and state the encryption method that is used.

☑ N/A

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

☑ N/A

Click here to select.

5.11 Does the project allow for the PII to be redisclosed by the external entities or require the external entities to request permission prior to its redisclosure? If so, describe the limitations on redisclosure and how they are documented and enforced.

☑ N/A

Click here to select.

6. Redress

6.1. What are the procedures that allow individuals to access their own information in the IT system? If there are no such procedures, state why not.

Individuals are able to access their information via phone through MIVA after verification of their identity.

Alternatively, if an individual wishes to gain access to a record in this system, that individual should provide the system manager with their name, DOB, and SSN.

Requests by an individual for access to a record must meet the requirements of the regulations in 34 CFR 5b.5, including proof of identity.

6.2. What procedures are in place to allow individuals to correct or amend inaccurate or erroneous information?

Information pertaining to mailing and email address can be updated through the MIVA HIVR. Other information must be corrected through ADVS; MIVA will deliver calls to an ADVS agent for this purpose.

Alternatively, if an individual wishes to amend the content of a record in this system of records, that individual should contact the system manager with their name, DOB, and SSN; identify the specific items to be changed; and provide a written justification for the change. Requests to amend a record must meet the requirements of the regulations in 34 CFR 5b.7.

6.3. How does the program or IT system notify individuals about the procedures for accessing or correcting their information?

If an individual wishes to determine whether a record exists regarding the individual in the system of records, that individual should provide the system manager with their name, DOB, and SSN. Requests must meet the requirements of the regulations in 34 CFR 5b.5 and 5b.7, including proof of identity.

7. Safeguards

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

7.1. Does the principal office work with their ISSO to build privacy and security safeguards into the IT system?

Yes

7.2. Is an authorization to operate (ATO) required for the IT system?

Yes

7.2.1. If the answer to Question 7.2 is **YES**, does the IT system have an active ATO?

Yes

7.3. What is the NIST Federal Information Processing Standard 199 security categorization of this IT system?

☐Low

☒Moderate

☐High

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

MIVA is a FedRAMP-authorized system hosted within the ADVS infrastructure. Access to the system is limited to ADVS employees and contractors. In accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and Office of Management and Budget (OMB) policy, servicers' systems must receive a signed authorization to operate (ATO) from a designated Department authorizing official. Security and privacy controls implemented for servicers' systems are comprised of a combination of administrative, physical, and technical controls. The system undergoes an assessment of management, operational, and technical security controls, plans of action and milestones (POA&Ms) to remediate any identified deficiencies, and a continuous monitoring plan. The MIVA Information System Security Officer (ISSO) is responsible for ensuring that the security posture is maintained for the system. All data in transit are encrypted; there are no data at rest on the system as information is stored within ADVS. ADVS employee access to the system requires unique user credentials to gain administrative access. FedRAMP requires the enforcement of a complex password policy and multi-factor authentication (MFA).

8. Auditing and Accountability

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

The system owner ensures that the information is maintained and used in accordance with the stated practices in this PIA by completing the Department Risk Management Framework process to receive an ATO. Furthermore, MIVA ensures that National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5 controls are implemented. The NIST controls are comprised of administrative, technical, and physical controls to ensure that information is used in accordance with approved practices. The system owner also participates in all major security and privacy risk briefings, meets regularly with the ISSO, and participates in FSA's Lifecycle Management Methodology, which address security and privacy risks through the system's lifecycle.

8.2. How does the ISO continuously monitor and audit the security and privacy controls to ensure effective implementation and safeguarding of PII?

MIVA participates in the Ongoing Security Authorization (OSA) Program and continuous monitoring program. The OSA, which reviews FISMA controls, is conducted quarterly, and the system is scanned continuously to ensure that security and privacy

controls are in place and working properly. MIVA has a regular patching cycle to ensure the system is secured with the most up-to-date capabilities. Following each patch release an additional scan is conducted to ensure continuing operations. In addition, security and privacy controls are monitored and updated regularly as required by FedRAMP. Several meetings per month are held to update controls. Controls are annually assessed and tested by an independent assessor. The system owner, in coordination with the ISSO and FSA assessment team, ensures the information is used in accordance with stated practices by confirming that the privacy risks are properly assessed, confirming the data are secured, ensuring appropriate security and privacy controls are implemented to restrict access, and properly managing and safeguarding PII maintained within the system.

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

Privacy risks associated with MIVA 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 per the patch scheduling and updating devices operating software, amongst other software. System patching is performed monthly, and 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.