



Privacy Impact Assessment (PIA)
for the

National Student Loan Data System (NSLDS)

May 25, 2022

For PIA Certification Updates Only: This PIA was reviewed on **May 25, 2022** by **Daniel Williams, ISO** and **Jeremy Dick, ISSO** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Jeremy Dick/Information System Security Officer
Contact Email: Jeremy.Dick@ed.gov

System Owner

Name/Title: Daniel Williams/Information System Owner
Principal Office: Federal Student Aid (FSA)

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 U.S. Department of Education's (Department) National Student Loan Data System (NSLDS) is a comprehensive legacy national database for the Federal financial aid history of recipients of student financial assistance and grants authorized under Title IV of the Higher Education Act of 1965, as amended (Title IV). As the central database for Title IV student financial aid, NSLDS stores information about loans, grants, students, borrowers, lenders, guaranty agencies (GAs), schools, and servicers. It provides detailed information on individuals pertaining to their Title IV loans and grants during all stages of their aid life cycle, from approval through disbursement, repayment, default, and closure.

The primary sources of information contained in NSLDS are other Federal Student Aid (FSA) systems, which include Common Origination and Disbursement (COD), Central Processing System (CPS), Debt Management Collections System (DMCS), Title IV Additional Servicers and Not for Profit Servicers (TIVAS/NFPs), and the Financial Management System (FMS). NSLDS also maintains records resulting from computer matching agreements (CMA) with the U.S. Department of Veterans Affairs (VA) for disability determination dates for any borrower who is a veteran and has received a VA disability compensation benefit or a determination that the veteran is totally disabled, the Social Security Administration (SSA) for Medical Improvement Not Expected disability status, and the U.S. Department of Defense (DoD) for active-duty status. It also supports real-time loan information exchanges with the U.S. Department of Health and Human Services (HHS) to allow HHS's Health Resources and Services Administration (HRSA) to make payments on outstanding applicant loans of health professionals working in a designated high-need area. All data sent into NSLDS by other FSA systems or Federal agencies is transmitted via encrypted protocols through the FSA Student Aid Internet Gateway (SAIG) system.

NSLDS runs on an IBM mainframe computer using an IBM database. NSLDS also contains two websites (nslsdfap.ed.gov and nslsdrain.ed.gov) that are used by schools, financial institutions, and loan servicers to review data and retrieve loan and grant information on borrowers. These websites use secure encrypted protocols for connection

to the mainframe database for retrieval and updates to borrower or loan information. Users accessing the websites are authenticated through the FSA Access and Identity Management System (AIMS) which uses two-factor authentication.

Borrowers can view their loan information through a secure connection after they sign on to studentaid.gov, which is a component of FSA’s Digital Customer Care (DCC) web portal. Borrowers are authenticated through the FSA Person Authentication Service (PAS) prior to accessing their data. The studentaid.gov website connects to NSLDS through a secure connection to retrieve the borrower’s data for viewing after the borrower is authenticated.

NSLDS also has a help desk to support data processing and questions from schools, loan servicers, and other institutions. Several validation programs are executed on data provided to NSLDS. The help desk assists callers in resolution of data validation errors and the corrections required for their data to be accepted and processed. Help desk agents access NSLDS through nsldsfp.ed.gov via a secure virtual private network (VPN) connection. Website access is provided so that help desk agents can review information that the school, institution, or servicer requesting assistance is seeing. Direct access to the system via personal identity verification (PIV) authentication is provided to the help desk so they can review processing status of caller’s data files sent to NSLDS.

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

NSLDS serves as the central database for Title IV student financial aid and stores information about loans, grants, students, borrowers, lenders, GAs, schools, and servicers. The system provides detailed information on individuals pertaining to their Title IV loans and grants during all stages of their aid life cycle, from approval through disbursement, repayment, default, and closure. The system also allows schools, financial institutions, and loan servicers to review data and retrieve loan and grant information on borrowers and grantees.

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

Currently Operating System

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](#)

1.4. 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.

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

Contractor

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

N/A

Yes

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.

NSLDS is authorized by Title IV of the Higher Education Act of 1965, as amended, and Executive Order 9397 as amended by Executive Order 13478.

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, SSN, date of birth, or loan ID.

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

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>

The SORN, entitled the “[National Student Loan Data System](#)” (18-11-06), 84 FR 47265-47271, was published in the Federal Register on September 9, 2019.

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.

[ED Records Schedule 051, National Student Loan Data System](#), covers records in the NSLDS. The disposition for these records is as follows: Cut off annually when account is paid in full. Destroy/delete 30 years 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?

No

NSLDS records are to be destroyed 30 years after repayment or discharge of the loan, per ED51. During the migration from the legacy NSLDS system to the NSLDS-New system, management has determined that removal of records so close to the migration would risk record validation inaccuracies and potential failures for conversion of data. The NSLDS Business owner submitted a formal exception to NARA with a firm date for destruction plan post conversion to the NSLDS on or before October 1, 2022, to retain records up to 48 months after the approved retention period of 30 years after cut-off. With the legacy system decommission on track for October 2022, adherence to the schedule will occur by March 31, 2023, in destructing eligible data from NSLDS.

The Department Records Officer, in coordination with the FSA Records Information Manager, is working on a Department-wide retention schedule, which will cover NSLDS records.

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.

Information collected from all aid recipients and applicants (and, if applicable, parents or spouses of aid recipients and prospective aid recipients) includes:

- Full name
- Social Security number (SSN)
- Date of birth
- Home or current address
- Home, work, and alternate telephone numbers
- Email address
- Driver's license number and State
- Citizenship status, dependency status, veteran status, marital status
- Gender
- Loan ID and loan or grant amount, disbursements, dates of disbursements, balances, repayment plan, loan status, collections, claims, deferments, forbearances, refunds, cancellations, overpayment amounts, and date of default
- Income information

Once aid is granted, the following information is also collected and stored from aid recipients:

- Educational enrollment information to include the educational institution Postsecondary Education identification number (OPEID number), the level of study, Classification of Instructional Programs (CIP) code, and program length
- Enrollment in a gainful employment program
- Course of study completion status and date
- Amount of the loan debt, the amount of institutionally provided financing owed by the student, and whether the student matriculated to a higher credentialed program at the same institution or another institution

Additionally, information on a borrower are obtained pursuant to matching programs from the following:

- SSA: Medical Improvement Not Expected disability status
- VA: Disability determination dates for any borrower who is a veteran and has received a VA disability compensation benefit or a determination that the veteran is totally disabled

- DoD: Active-duty status

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

Yes

The PII collected and maintained is the minimum amount required by NSLDS. NSLDS utilizes PII to uniquely identify individuals that receive aid under the Title IV of the Higher Education Act and to track the status of their loans and grants throughout the aid life cycle which includes application, origination and disbursement of funds, and servicing and repayment history.

NSLDS requires the PII to uniquely identify individuals that receive aid under the Title IV of the Higher Education Act and to track the status of their loans and grants throughout the aid life cycle which includes application, origination and disbursement of funds, and servicing and repayment history. Additionally, NSLDS is used by institutions of higher education to view the loan status of borrowers which require the use of PII to uniquely identify them.

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

The primary sources of information contained in NSLDS are from other FSA systems, which include COD, CPS, DMCS, TIVAS/NFPs, and the FMS.

NSLDS also maintains records that the Department obtains as a result of CMAs with three Federal agencies: (1) VA for disability determination dates for any borrower who is a veteran and has received a disability compensation benefit or a determination that the veteran is totally disabled, (2) SSA for Medical Improvement Not Expected disability status validation, and (3) DoD for active-duty status.

All data sent into NSLDS by other FSA systems or Federal agencies are transmitted via encrypted protocols through the FSA Student Aid Internet Gateway (SAIG) system.

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

Internal and external systems send data to NSLDS electronically through the FSA SAIG system for processing and reporting.

- 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?

PII is received from other FSA systems, as described above. Please refer to the PIAs for the other Department systems to understand how those systems validate the PII. In addition, other information is provided by other Federal agencies as part of computer matching programs to help verify the accuracy of the records. The system maintains detailed information on individuals pertaining to their Title IV loans and grants during all stages of their aid life cycle, from approval through disbursement, repayment, default, and closure. If an individual or institution notes the PII that FSA maintains about them is incorrect, records are updated within the system, as detailed in question 6.2.

Use

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

NSLDS uses PII to track borrowers throughout the student aid lifecycle, as individuals transition through attendance at an institution of higher education to repayment of loans. NSLDS consolidates information from multiple FSA systems to maintain an official record of the individual to support the student aid lifecycle.

NSLDS also maintains records resulting from CMAs with the VA for disability determination dates for any borrower who is a veteran and has received a VA disability compensation benefit or a determination that the veteran is totally disabled, the SSA for Total Permanent Disability validation, and the DoD for active-duty status. It also supports real time loan information exchanges with the HHS to allow HHS's HRSA to make payments on outstanding applicant loans of health professionals working in a designated high-need area.

- 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

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.

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 collected to uniquely identify aid recipients and support the multiple data exchanges with systems that rely on the SSN to identify borrowers. NSLDS utilizes SSNs and date of birth to match records with other Federal agencies supported by CMAs.

- 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 but were determined to not be feasible given the design of systems at FSA and other Federal agencies, as well as the lack of a consistently collected alternative identifier that is capable of performing the same function as the SSN. FSA's data exchanges rely on SSN and date of birth to identify and track aid recipient's loans, grants, and 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.

NSLDS is part of the Student Aid Lifecycle where privacy notice is given at the point of collection on the Free Application for Federal Student Aid (FAFSA) electronic form and other loan or grant applications. In addition to the notice given at the point of collection,

NSLDS also provides additional general notice through the privacy policy on the studentaid.gov website.

- 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

<https://studentaid.gov/notices/privacy>

- 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?

Providing information to FSA is voluntary. However, NSLDS is part of the student aid lifecycle and, once individuals provide information to FSA via other FSA systems, individuals do not have the ability to specifically decline to have their information maintained in NSLDS. Opportunities to decline to provide PII or opt out are at the initial point of collection on the FAFSA or at other points of collection (e.g., at the VA, SSA, or DoD). If individuals decline to provide PII, that may prevent the individuals' student aid application from being submitted or processed and affect the possibility of receiving student aid.

- 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

NSLDS records are shared with the Department's Office of the Inspector General's (OIG) Data Analytic System (ODAS).

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

N/A

Records are shared with OIG to assist in identifying fraud. For more information on the uses of ODAS, please refer to the PIA for ODAS.

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

NSLDS shares name, SSN, and date of birth with the SSA, VA, and DoD pursuant to CMAs.

NSLDS maintains and shares records resulting from CMAs with the VA for disability determination dates for any borrower who is a veteran and has received a disability compensation benefit or a determination that the veteran is totally disabled, the SSA for Medical Improvement Not Expected disability status validation, and the DoD for active-duty status.

Information regarding loan status for participants in student loan repayment programs will be shared with HHS to allow HHS's HRSA to make payments on outstanding applicant loans of health professionals working in a designated high-need area.

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

N/A

See question 5.5.

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.

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

All data shared by NSLDS to other Federal agencies is transmitted via encrypted protocols through the FSA SAIG system.

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?

If an individual requires access to their records maintained in NSLDS they may obtain access by logging into their online account through studentaid.gov or their Federal loan servicer.

Additionally, if the individual wishes to gain access to a record in this system, they may contact the system manager with the necessary particulars such as name, date of birth, SSN, the name of the school or lender from which the loan or grant was obtained, and any other identifying information requested by the Department while processing the request, to distinguish between individuals with the same name. Requests by an

individual for access to a record must meet the requirements of the regulations at [34 CFR 5b.5](#), including proof of identity.

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

To correct inaccurate or erroneous information, individuals can log into their online account through [studentaid.gov](#) or their Federal loan servicer.

Additionally, if an individual wishes to contest the content of a record in the system of records, they must contact the system manager with the necessary particulars such as name, date of birth, SSN, the name of the school or lender from which the loan or grant was obtained, and any other identifying information requested by the Department while processing the request, to distinguish between individuals with the same name. You must also identify the specific item(s) to be changed, and provide a justification for the change, including any supporting documentation. Requests to amend a record must meet the requirements of the Department's Privacy Act regulations at [34 CFR 5b.7](#).

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

The SORN listed in question 2.2.1 and this PIA explain 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 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?

Access to the system is limited to authorized NSLDS program personnel and contractors responsible for administering the NSLDS program. Authorized personnel include Department employees and contractors, including financial and fiscal management personnel, computer personnel, and program managers who have responsibilities for implementing the NSLDS program.

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), NSLDS must receive a signed ATO from a designated FSA official. FISMA controls implemented by NSLDS are comprised of a combination of management, operational, and technical controls. All users have a specific role assigned to them approved by the Information System Security Officer (ISSO), are required to read and accept a Rules of Behavior and are required to utilize a complex password and two-factor authentication.

Physical safeguards include the staffing of security guards 24 hours a day, seven days a week, to perform random checks on the physical security of the record storage areas. All sensitive data are encrypted in transit and at rest, access to records is strictly limited to those staff members trained in accordance with the Privacy Act and Automatic Data Processing (ADP) security procedures.

- 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.

Weekly scans are performed in support of code migrations and/or system fixes. Quarterly authenticated network and operating vulnerability scans, along with network

penetration testing, are conducted to ensure the security of the NSLDS network environment. As part of an ongoing security and authorization process, security audits are performed on an annual basis by authorized independent third parties to ensure the controls in place are effectively securing our data. NSLDS is required to submit Plans of Actions and Milestones (POA&MS) to FSA quarterly which continuously monitor any vulnerabilities and ensure that they are mitigated and closed. Additionally, self-assessments are conducted annually.

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 ensures that the information is maintained and used in accordance with the stated practices in this PIA.

The first method is by completing the Department's risk management framework process to receive an ATO. During the ATO process, NSLDS makes sure that the National Institute of Standards and Technology (NIST) Special Publication 800-53 controls are implemented. The NIST controls comprise of administrative, technical, and physical controls to ensure that information is used in accordance with approved policies and practices.

The system owner ensures the information is used in accordance with stated practices by confirming that the privacy risks are properly assessed, and the data are secured, ensuring appropriate security and privacy controls are implemented to restrict access, and to properly manage and safeguard PII maintained within the system. The system owner participates in all major security and privacy risk briefings, meets regularly with the ISSO, and participates in FSA's Lifecycle Management Methodology (LMM), which addresses security and privacy risks throughout the system's life cycle. Additionally, the system owner regularly reviews signed agreements that govern data use between organizations, such as information sharing agreements and memoranda of understanding.

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 NSLDS 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 granting access to only authorized individuals based on their respective position and on a need-to-know basis, limiting users to those who are screened, utilizing least privilege principles, masking SSNs, and encrypting data in transmission. Risks are also mitigated by updating security patches per the patch scheduling and updating devices' operating software, amongst other software. As referenced above, patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle.