Privacy Impact Assessment (PIA)

for the

FSA Cloud (NextGen General Support System (GSS))

September 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: Corey Johnson, Information System Security Officer (ISSO)
Contact Email: Corey.Johnson@ed.gov

System Owner

Name/Title: Diana O'Hara, Production Division Director
Principal Office: Federal Student Aid

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 Federal Student Aid (FSA) Cloud is a hybrid cloud infrastructure located on various network and cloud-based operating system platforms and includes the infrastructure, security and network components that support the Digital and Customer Care (DCC) application platform. The FSA Cloud is hosted in an Accenture contracted Amazon Web Services (AWS) cloud. The AWS cloud is FedRAMP-approved and is authorized to host PII. FedRAMP is a U.S. government-wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud services. The FSA Cloud is described as an Information Management Solution (IMS) infrastructure. The IMS infrastructure includes Local Area Networks (LANs), Virtual Local Area Networks (VLANs), Wide Area Networks (WANs), servers, networks, AWS US East, Salesforce and, AWS Gov Cloud services, and other IT components.

Hardware and software components within the IMS are hosted at various locations including: MTIPS, NTTA, Ashburn, VA; NTTA, Dallas, TX, Contact Center Backbone (CCB), Union Center Plaza (UCP) Command Center, Washington DC via NTTA, AWS GovCloud West, and, AWS GovCloud East. The Training Portal is hosted in the Oracle Taleo Cloud.

The FSA Cloud will be a temporary storage location for National Student Loan Data System (NSLDS) data while the NSLDS data is converted into Oracle database format and as part of the development effort for the new NSLDS which will be hosted as a tenant in the FSA Cloud. This conversion is part of the overall FSA NextGen project which is expected to occur into late 2021. While the data is located in the FSA Cloud, the existing NSLDS will continue operations until to the new system is ready for operations. There will be no data processing or communications with external entities from the new system until the new system is ready for operations.

NSLDS is the first comprehensive national database of information about the Federal financial aid history of recipients of student financial assistance authorized under Title IV of the Higher Education Act of 1965, as amended. As the central database for Title IV student financial aid, the NSLDS stores information about loans, grants, students,

borrowers, lenders, guaranty agencies (GAs), schools, and servicers. It provides an integrated view of Title IV loans and grants during all stages of their life cycle-from aid approval through disbursement, repayment, default, and closure.

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

NSLDS, and temporarily, the FSA Cloud, serves as the centralized repository for all records throughout the Student Aid Lifecycle. All FSA systems that are part of the lifecycle report to NSLDS in order to maintain a comprehensive identity of a borrower and track their loans from disbursement through closure. NSLDS maintains PII in order to ensure there is an authoritative source for a borrower's identity. Additionally, NSLDS is used by institutions of higher education to view the loan status of borrowers.

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

Currently Operating System	The currently operating system is NSLDS.

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

New PIA	A new PIA was needed to account for the temporary storage of NSLDS data in the FSA Cloud.

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

[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

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.

Title IV of the Higher Education Act of 1965, as amended, and Executive Order 9397 as amended by Executive Order 13478. This law authorizes FSA to manage the student financial assistance programs authorized under Title IV of the Higher Education Act of 1965. These programs provide grant, work-study, and loan funds to students attending college or career school.

The collection of Social Security numbers (SSNs) of borrowers who are covered by this system is authorized by 31 U.S.C. 7701 and Executive Order 9397 (November 22, 1943), as amended by Executive Order 13478 (November 18, 2008), which allows ED to collect SSNs in order to administer FSA programs.

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

National Student Loan Data System, published in the *Federal Register* on September 9, 2019 at 84 FR 47265-47271.
https://www.federalregister.gov/documents/2019/09/09/2019-19354/privacy-act-of-1974-system-of-records

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.

[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

☑ 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.

ED Records Schedule 051, National Student Loan Data System, covers records in the NSLDS. The disposition for these records is as follows: Cutoff annually when account is paid in full. Destroy/delete 30 years after cutoff. A cutoff is when a record series is divided into blocks in order to apply the disposition. This involves ending the old files and starting new ones at regular intervals. The retention period is then applied at the cutoff point.

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 NSLDS 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;

Educational enrollment information for the borrower such as the educational institution, level of study, Classification of Instructional Programs (CIP) code, and program length; In addition to the educational enrollment information above, if student is enrolled in a gainful employment program, additional information will include the Office of Postsecondary Education identification number (OPEID number) of the institution, the student's completion status and date, the amount of the student's private educational 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;

Information obtained pursuant to matching programs, which includes Medical Improvement Not Expected disability status from the Social Security Administration (SSA) and disability determination dates for any borrower who is a veteran and has received a Department of Veterans Affairs (VA) disability compensation benefit or a determination that the veteran is totally disabled.

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

Yes

NSLDS collects only the minimum information necessary to administer the program. Contact information is needed to communicate with the recipients and administer the program. Additional information, such as SSNs, is needed to track borrowers throughout the student aid lifecycle and identify the student. PII is also collected pursuant to computer matching agreements with the Social Security Administration and the Veteran's Administration. 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.)?

The primary source of the information in NSLDS is other internal FSA systems such as Common Origination and Disbursement (COD), Central Processing System (CPS),

Digital Customer Care (DCC), Debt Management Collections System (DMCS), Title IV Additional Servicers and Not for Profits (TIVAS/NFPS), Financial Management System (FMS), FSA Information Center (FSAIC), and Student Aid Internet Gateway, Participation Management (PM). For more information on these and the PII maintained in them, please reference the corresponding PIAs and SORNs.

NSLDS also maintains records resulting from Computer Matching Agreements (CMA) with the Department of Veteran's Affairs (VA) and the Social Security Administration (SSA).

PII is also sourced from schools, the individual borrower, and guaranty agencies or their servicers.

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

Schools, Guaranty Agencies, Federal Loan servicers, borrowers and other Federal Agencies send data to NSLDS electronically through the Student Aid Internet Gateway (SAIG) or encrypted electronic exchange mechanisms 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?

The NSLDS data Quality Management functions consists of proactive analysis of all data inputs, data processing, and data outputs. This includes standard documentation provided to data submitters (Data Provider Instructions (DPI)) and feedback from the NSLDS online systems as to appropriate input values. All computer program or website software changes to the online and batch systems are peer reviewed, internally tested, and Quality Assurance tested prior to introduction into the system. Many reports are available to help the data providers, as well as FSA, identify and document data quality on a regular basis.

The approach to data management on NSLDS focuses on two key areas of Data Quality. The first area is the quality of data being reported or data entered into the system. This includes software that validates the data with edits and error reports prior to updating

[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.

data in the system. The second area is database quality and consistency within the system's database tables and how data is stored once it has been entered into the system. The NSLDS Data Quality (DQ) team is led by the Database Administrator, DQ manager, and Data Integrity Group.

The objectives of the Data Quality team are: (1) To identify and summarize the data quality of the inputs, processing, and outputs of NSLDS. Inputs to the database include multiple items such as data provider data submissions and online updates including uploads of data. Processing of the data includes program and data consistency checks. Outputs include reports, website page accuracy, and ad-hoc data requests. (2) Monitoring and maintaining the levels of accuracy and reliability of NSLDS data for continuing improvement. This work includes establishing data quality benchmark goals and continually measuring
improvements.

Use

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

NSLDS uses PII to identify borrowers and track their loan and grant information throughout the student aid lifecycle, as individuals transition through attendance at an institution of higher education to repayment of loans. NSLDS is the authoritative source of an individual's receipt of Federal funds for loans and grants across the multiple FSA systems that support the lifecycle.

Additionally, PII is used pursuant to computer matching agreements with the Social Security Administration and the Veteran's Administration in order to obtain additional information on the disability status of borrowers and Veterans to determine loan forgiveness, or to adjust repayment schedules.

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

Social Security Numbers (SSN) are collected because the NSLDS interfaces with multiple institutional, servicing, and external Federal Agency systems that rely on the SSN to identify borrowers. NSLDS utilizes SSNs to match records maintained in other Federal systems in the course of matching pursuant to a Computer Matching Agreement with other Federal agencies.

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. The alternatives have not been selected because the NSLDS interfaces with multiple systems that rely on SSN to identify students, loans, grants, and over-payments. No alternative identifier would suffice to allow FSA to achieve its authorized functions.

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 a privacy notice is given at the point of collection on the Free Application for Federal Student Aid (FAFSA) and other loan or grant applications. This is provided through a Privacy Act Statement. The Privacy Act Statement describes the Department's authority for the collection of PII, the principal purposes for which PII will be used, the published routine uses of the PII, and the consequences of not providing all or part of the requested information. When additional

information is collected directly from the individual, additional notice is provided through the use of 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

http://nsldsfap.ed.gov/nslds_FAP/
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 is voluntary. Individuals have an opportunity to decline to provide PII at the initial point of collection. However, NSLDS is part of the Student Aid Lifecycle, and once individuals have provided their information, they do not have the ability to revoke consent or opt out of their information being maintained in NSLDS.

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 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 Office of Inspector General Data Analytic System (ODAS), please refer to the Office of Inspector General Data Analytic System (ODAS) PIA which can be found on the U.S. Department of Education Privacy Impact Assessment (PIA) page.

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 Social Security Administration pursuant to a Computer Matching Agreement.

PII may also be shared with guaranty agencies, educational institutions, financial institutions and their servicers, Federal and State agencies, government researchers at the Federal, State, and local level, the Congressional Budget Office (CBO), the Department of Justice (DOJ), SSA, and the Department of the Treasury pursuant to a programmatic disclosure published as a routine use in the SORN referenced in 2.2.1.

Information regarding loan status for participants in student loan repayment programs will be shared with requesting entities such as the Department of Health and Human Service's (HHS) Health Resources and Service Administration (HRSA) and New York State's Get on Your Feet Program (GOYF).

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

☐ N/A

PII is shared with SSA to identify individuals who are eligible for a Total and Permanent Disability (TPD) discharge of their Title IV Loans or TEACH Grant Service Obligations. The Department can proactively reach out to individuals informing them of

[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.

their eligibility. For more information on this computer match please reference the CMA found here: https://www2.ed.gov/about/offices/list/om/pirms/cma.html
PII may be disclosed pursuant to one of the following programmatic disclosures published as a routine use in the SORN referenced in 2.2.1.
• To verify the identity of the applicant involved, the accuracy of the record, or to assist with the determination of program eligibility and benefits, to assist in locating loan holders or loan borrowers,
• To support default rate calculations and/or provide information on borrowers' current loan status,
• To provide financial aid history information to aid in the administration of title IV, HEA programs,
• To support governmental researchers, policy analysts, auditors, program reviewers, Federal budget analysts
• To assist with meeting requirements under the Credit Reporting Act and in tracking loans funded under Ensuring Continued Access to Student Loans Act
• To assist program administrators with tracking refunds and cancellations of title IV, HEA loans,
• To enforce the terms of a loan, assist in the collection of a loan, or assist in the collection of an aid overpayment,
• To assist the Department in complying with requirements that limit eligibility for Direct Subsidized Loans, and to determine when a borrower will be responsible for the interest accruing on outstanding Direct Subsidized Loans,
• To obtain data needed to assist the Department in evaluating the effectiveness of an institution's education programs and to provide the public with greater transparency about the level of economic return of an educational institution and their programs that receive title IV, HEA program assistance and determine if educational programs lead to gainful employment in a recognized occupation.
PII is shared with the consent of the loan holder to HHS-HRSA and NY GYOF for the purposes of supporting student loan repayment programs.

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 with external entities via encrypted electronic transmission.

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 The data being stored in the FSA Cloud is only temporary and it will not be updated or used for any NSLDS processing until after the new NSLDS is developed, tested and implemented at which time the existing NSLDS will be decommissioned. The existing NSLDS will stay in operations and be used for processing changes and updates to all of the data.

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

☐ N/A

Yes None of the temporarily stored data will be used in processing changes or disclosed. Please see answer to 5.10.

6. Redress

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

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

Additionally, if an individual wishes to gain access to their records in NSLDS, they can contact the system manager listed in the SORN listed in section 2.2.1 of this document and provide their name, date of birth, SSN, and the name of the school or lender from which their loan or grant was obtained.

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, individuals may contact their institution of higher education or, as a last result, the Office of the Ombudsman to have inaccurate or erroneous information corrected in NSLDS.

Finally, if an individual requests amendment of their records in NSLDS, they can contact the system manager listed in the SORN listed in section 2.2.1 of this document and provide their name, date of birth, SSN, and the name of the school or lender from which their loan or grant was obtained.

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

The system of records notice listed in question 2.2.1 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?

Access to the FSA Cloud which is hosting the new NSLDS solution is limited to authorized contractor and FSA staff working on the NSLDS data conversion and re-platforming effort. Authorized personnel include Department employees, IT professionals working on the technical solutions for rehosting NSLDS and FSA and contractor program managers who have responsibilities for establishing the new NSLDS hosting environment, converting NSLDS data, and developing and testing the new NSLDS solution. In accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and Office of Management and Budget policy,

FSA Cloud must receive a signed Authorization to Operate (ATO) from a designated ED authorizing official. Security and privacy controls implemented by FSA Cloud are comprised of a combination of administrative, physical, and technical controls.

Moreover, FedRAMP requirements include additional controls above the standard NIST baseline controls in NIST SP 800-53 Revision 4. These additional controls address the unique elements of cloud computing to ensure all federal data is secure in cloud environments.

Physical access to the sites of the Department's contractors, where this system is maintained, is controlled and monitored by security personnel who check each individual entering the buildings for his or her employee or visitor badge. All contract and Department personnel who have facility access and system access must undergo a security clearance investigation. Individuals requiring access to information subject to the Privacy Act of 1974 are required to hold, at a minimum, a moderate-risk security clearance level. These individuals are required to undergo periodic screening at five-year intervals. In addition to undergoing security clearances, contract and Department employees are required to complete security awareness training on an annual basis. Training is required to ensure that contract and Department users are appropriately trained in safeguarding these data. The computer system employed by the Department offers a high degree of resistance to tampering and circumvention through the application of security controls. These controls limit data access to Department and contract staff on a "need-to-know" basis and control individual users' ability to access and alter records within the system.

All users accessing the system are given unique user identification. The Department requires the enforcement of a complex password policy and two-factor authentication. In addition to the enforcement of the complex password policy, users are required to change their password at least every 90 days in accordance with the Department's information technology standards. Physical security of electronic data will be maintained in a secured data center, access to which is controlled by multiple access controls. Cryptographic solutions are in place to prevent unauthorized disclosure of information and to protect the integrity of data at rest and in transit.

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 is conducted to ensure the security of the FSA Cloud network environment. As part of an ongoing security and authorization process, security audits are performed on a quarterly and annual basis by authorized independent third parties to ensure the controls in place are effectively securing our data. Security staff for the FSA Cloud are required to submit Plans of Actions and Milestones 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 the information is used in accordance with stated practices by confirming the privacy risks are properly assessed, ensuring Privacy Act records are maintained in accordance with the provisions of the Federal Records Act, Departmental policies, the Privacy Act, and the published SORN, ensuring appropriate security and privacy controls are implemented to restrict access, and to properly manage and safeguard PII maintained within the system. These actions are regularly performed according to documented, specified procedures. The system owner participates in all major security and privacy risk briefings, meets regularly with the Information System Security Officer, and participates in FSA's Lifecycle Management Methodology (LMM), which addresses security and privacy risks throughout the system life cycle. Additionally, the system owner regularly reviews signed agreements that govern data use between organizations, such as memoranda of understanding and Computer Matching Agreements.

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?

This PIA details the privacy controls and safeguards implemented for this system in order to mitigate privacy risk. These controls and safeguards work to protect the data from privacy threats and mitigate the risks to the data.

One key privacy risk associated with NSLDS is unauthorized access, use, or disclosure of PII pertaining to borrower/co-borrower/and students. These data breaches involving PII can be hazardous to individuals because they can result in identity theft or financial fraud. Risks to the Department in such an event would result in embarrassment, loss of public trust, and the cost to the Department of providing remedial actions such as credit monitoring.

The risks are mitigated by the above-mentioned controls and safeguards, updating the security patches and software throughout a continuous monitoring process, limiting access to NSLDS to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department.

Another risk is that, because the information is hosted in an external cloud environment, there are security risks that do not exist in the NSLDS system. In order to mitigate that risk, the FSA Cloud has been assessed along with other tenants one of which is Digital Customer Care that is a system hosted in the FSA cloud and the front-end entry point for borrowers to access information on their loans and grants to ensure adequate controls are in place. As part of the assessment, the FedRAMP AWS Gov Cloud package was reviewed and certified for use by the Department. Moreover, FedRAMP requirements include additional controls above the standard NIST baseline controls in NIST SP 800-53 Revision 4. These additional controls address the unique elements of cloud computing to ensure all federal data are secure in cloud environments.