



## **Privacy Impact Assessment**

For Department of ED/Perkins (DOED Perkins)

DOED Perkins Loan Servicing System

**Date:** January 13, 2016

**Point of Contact:**

Calvin Whitaker

202.377.3045

[Calvin.whitaker@ed.gov](mailto:Calvin.whitaker@ed.gov)

**System Owner:**

Diana O'Hara

202.377.3466

[Diana.OHara@ed.gov](mailto:Diana.OHara@ed.gov)

**Author:**

Calvin Whitaker

**Office of Federal Student Aid**

**U.S. Department of Education**



1. **System Information.** Describe the system - include system name, system acronym, and a description of the system, to include scope, purpose and major functions.

The Department of Education Perkins Loan Servicing System (DOED Perkins) is an information system that handles loan servicing functionality for the Federal Student Aid (FSA) Program Office within the DOED. The system is managed by Educational Computer Systems Incorporated (ECSI), a Loan Servicing company located in Pittsburgh, Pennsylvania. The operational capabilities of the system include borrower account management, loan conversion/de-conversion, interim repayment servicing, payment posting, deferment and forbearance processing, borrower correspondence; call scheduling, collection, skip-tracing and correspondence history files. The DOED Perkins Loan Servicing system communicates with the internal FSA platforms, borrowers, other loan servicers, third-party data providers, consumer reporting agencies, guarantors and government agencies (as permitted by the Federal Privacy Act of 1974). Channels of communication include U.S mail, telephone calls, a secure borrower website, secure email and secure data transfer links.

2. **Legal Authority.** Cite the legal authority to collect and use this data. What specific legal authorities, arrangements, and/or agreements regulate the collection of information?

The Higher Education Act of 1965, as amended Section 441 and 461 Title IV, Section 401.

3. **Characterization of the Information.** What elements of personally identifiable information (PII) are collected and maintained by the system (e.g., name, social security number, date of birth, address, phone number)? What are the sources of information (e.g., student, teacher, employee, university)? How is the information collected (website, paper form, on-line form)? Is the information used to link or cross-reference multiple databases?

The DOED Perkins system collects and maintains the following elements of PII:

- Full name
- Maiden name
- Social Security Number (SSN)
- Bank Account number
- Student loan account number
- Driver license number and State
- Alien registration number
- Date of Birth (DOB)
- Home address
- Home, work, alternate and mobile telephone numbers
- Financial information
- Email addresses
- Employment information
- Related demographic data
- Medical information (to the extent required for purposes of certain deferments and discharge requests)

Borrower loan information including: disbursement amount, principal balance, accrued interest, loan status, repayment plan, repayment amount, forbearance status, separation date, grace period and delinquency status.

The information is obtained from the student/borrower, co-borrowers, co-signers, references provided by the borrower, educational institutions, financial institutions, employers, US National



Student Clearinghouse (NSC) and external database (e.g. Directory Assistance, consumer reporting agencies, skip-tracing vendors, U.S Military (all branches), commercial person locator servicers and U.S. Department of the Treasury).

The information is collected via the following channels:

- Phone calls with customers service agents
- Entries via the Interactive Voice Response (IVR) service
- Incoming correspondence (e.g. via U.S mail, email, etc.)
- Entry via Borrower Portal Web site. Refer to question 10 hereof.
- Bulk file transfer from third-party data providers as required, secure data transmission from
- DoED applications, such as: NSLDS and Debt Management Collection System (DMSC), etc.
- Secure data transmission from the U.S. Department of the Treasury.

The information is used in connection with loan processing and servicing activities, such as identity verification and authentication during online account creation and telephone calls, verification between internal databases within the DOED Perkins system and data exchange with external trading partners databases, such as:

- Consumer reporting agencies
- Lending institutions and other loan servicer
- Directory Assistance
- National Change of Address (NOCA) system
- Educational Institutions.

**4. Why is the information collected?** How is this information necessary to the mission of the program, or contributes to a necessary agency activity? Given the amount and any type of data collected, discuss the privacy risks (internally and/or externally) identified and how they were mitigated.

The information is necessary to uniquely identify borrowers and to service their student loans on behalf Federal Student Aid. The DOED Perkins database assists in tracking information pertinent to the borrower as well as information needed to process and service student loans throughout the loan lifecycle. Collection of this information protects FSA's interest by supporting timely and full repayment of loans and enables DOED Perkins to assist borrowers with managing their loans. The information is also needed to determine borrower eligibility for entitlements such as deferments, forbearances, discharges and to locate borrowers in cases of invalid addresses and/or telephone numbers. The servicing of student loan functions entails the following:

- Verifying loan details
- Mailing of forms for loan forbearances, deferments and repayment option modifications
- Mailing/emailing of statements of accounts
- Mailing of change of address inquires
- Verifying identify for account management
- Identifying and verifying borrowers during loan conversion/de-conversion
- Scheduling due diligence calls
- Issuing loan discharge and forgiveness claims and correspondence



- Maintaining and preparing loan and account history records and reports
- Planning for audit and program reviews
- Optimizing internal processes
- Transmitting loan information to FSA loans central processing platform via DOED applications such as NSLDS, DMCS, and Total Permanent Disability (TPD).

The privacy risks would result from a breach of DOED Perkins and ECSI's security safeguards as implemented on the DOED Perkins system, which could compromise the confidentiality, integrity and availability of information. The most likely method of breach would be through unauthorized access that would enable an adversary to disclose, damage the integrity of or prevent the availability of information. Another type of risk would be a man-made or natural disaster destroying the data center or place of business. These risks are mitigated by a robust security posture and strong controls, detailed below in question 11. Risk have additionally been mitigated by only collecting the minimum necessary amount of data, using the data only for the purpose for which is was collected, and disclosing the information only as allowed by law and for legitimate business purposes.

Key Risk Mitigation Measures include:

- Physical security, such as guards, access badges and security cameras protect against unauthorized access to component facilities.
  - Unauthorized access to the system itself is addressed by network intrusion detection systems, firewall/firewall log monitoring, malware detection and removal software, Virtual Private Networks (VPN) and encryption at the perimeter.
  - All external electronic transmissions used to receive or end PII data are encrypted.
  - To protect unauthorized access to DOED Perkins and ECSI employees, audit logs are maintained and reviewed at regular intervals and DOED Perkins system access is restricted by limiting the access based on the principle of least privilege.
  - Unauthorized system use by DOED Perkins and ECSI employees is subject to strict penalties.
  - All DOED Perkins and ECSI personnel are required to obtain government security clearances, to read and acknowledge the Rules of Behavior and to complete an initial security training and awareness course as well as periodic refresher training.
  - All DOED Perkins and ECSI infrastructure is located in facilities that leverage appropriate environmental controls.
  - DOED Perkins and ECSI maintain appropriate systems for redundancy and failover.
  - Borrowers accounts accessed via the secure website require multi-factor authentication.
  - DOED Perkins and ECSI maintain incident response, disaster recovery and business recovery plans to minimize impact of any failure/outages from mad-made or natural disasters.
  - DOED Perkins ECSI requires annual security training for all employees and implements security controls as mandated by the Federal Information Security Management Act (FISMA). Implementation of these controls and associated risks and mitigation is reflected in required security documentation. Additionally information regarding risk mitigation and security safeguards is provided in Section 11.
5. **Social Security Number (SSN).** If an SSN is collected and used, describe the purpose of the collection, the type of use, and any disclosures. Also specify any alternatives that you considered, and why the alternative was not selected. If system collects SSN, the PIA will



require a signature by the Assistant Secretary or designee. If no SSN is collected, no signature is required.

The SSN is the unique identifier for Title IV programs and its use is required by program participants and their trading partners to satisfy borrower eligibility, loan servicing and loan status reporting requirements under law and regulations. Trading partners include the Department of Education, Internal Revenue Service (IRS), and institutions of higher education, National Credit Bureaus, lenders and servicers.

The DOED Perkins system uses the SSN for the following functions:

- To verify identity and determine eligibility to receive a benefit on a loan (such as deferment, forbearance, discharge or forgiveness)
- As a unique identifier in connection with the exchange of information between the DOED Perkins system and its trading partners (e.g. educational institutions, financial institutions, loan services and consumer reporting agencies) that is performed in association with the servicing of the loan
- As a data component for submission of loan data to DoED, NSLDS and Tax Form 1098-E data to the IRS
- To locate the borrower and to report and collect on the loan in case of delinquency or default.

DOED Perkins assigns a unique account number to each borrower that is used to communicate with the borrower in lieu of the SSN. The borrower has the option to use DOED Perkins's System account number in place of the SSN during the identification process when communicating with DOED Perkins and interacting within the DOED Perkins system. In the event the borrower chooses to use the SSN, the DOED Perkins system uses the SSN for the following function:

- To verify borrower identity when establishing an online account with the DOED Perkins system. Once the account is created, the borrower receives a User ID and password, which are used for future authentication when using the DOED Perkins system borrower portal.
- To identify borrowers who call into the IVR or customer service call center.

This unique account number is not an accepted identifier with trading partners or third-party data Platforms that interface with the DOED Perkins system; the SSN is required for these types of transactions.

- 6. Uses of the Information.** What is the intended use of the information? How will the information be used? Describe all internal and/or external uses of the information. What types of methods are used to analyze the data? Explain how the information is used, if the system uses commercial information, publicly available information, or information from other Federal agency databases.

The information is collected and maintained to enable DOED Perkins to perform FSA business related to student loans and it's necessary to adequately service and ensure successful collection of loans.



The DOED Perkins system will employ the information to support the following capabilities:

- Support for its student loan servicing function. Operational capabilities include loan conversion/de-conversion, interim/repayment, servicing, repayment posting, deferment and forbearance processing, letter generation, call scheduling, collection, skip-tracing, claims and correspondence history files.
- Provide three major forms of account management and customer access for borrowers. The DOED Perkins system currently provides a secure website where the borrower can access account information and conduct specific loan transactions. The borrower can also place calls for self service via the IVR or to live customer service agents where the full range of loan services are provided. Finally, the borrower can also mail in forms and other correspondence to the DOED Perkins system.

External uses of the information include:

- Reporting to consumer reporting agencies for purposes of credit reporting
- Reporting to Directory Assistance to verify telephone numbers
- Exchanging information held by the NSC and educational institutions for purposes of educational data and address verification
- Exchanging information held by the U.S. Postal database for purposes of checking the validity of zip codes entered and validating address updates
- Exchanging information with skip-trace vendors for purposes of verifying/obtaining updated borrower contact information
- Providing information to NSLDS, which is used by educational institutions for the purposes of determining eligibility for programs and benefits
- Exchanging information with person locator servicers, which may be used during skip-tracing and collection activities in order to locate the borrower or collect payments.

The data can be analyzed by system processes and by DOED Perkins and ECSI employees. Specific methods used include manual calculations and analysis of data using desktop query tools and SAS (Statistical Analysis System).

**7. Internal Sharing and Disclosure.** With which internal ED organizations will the information be shared? What information is shared? For what purpose is the information shared?

In accordance with requirements set forth by DoED, the DOED Perkins system shares information with DoED to allow it to administer the Direct Loan Program. DoED may disclose information contained in a record in an individual's account in accordance with the Privacy Act of 1974. DOED Perkins shares information with:

- Federal Student Aid and its agents or contractors
- National Student Loan Data System (NSLDS)
- Debt Management Collection System (DMCS)
- Total and Permanent Disability System (TPD)
- Common Origination and Disbursement System (COD)
- Student Aid Internet Gateway (SAIG)



Please refer to question 4, which describes what information is shared, for what purpose the information is shared, the risk to privacy for internal sharing and disclosure and how the risks are mitigated.

8. **External Sharing and Disclosure.** With what external entity will the information be shared (e.g. another agency for a specific programming purpose)? What information is shared? For what purpose Is the information shared? How is the information shared outside of the Department? Is sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU) or other type of approved sharing agreement with another agency?

All information described in question3 hereof may be shared with external entities. DOED Perkins will be required to interface and share information with the following non-Department of Education systems and government entities.

- IRS (including Adjusted Gross Income requests, waivers image processing and 1098E/1099)
- U.S. Department of Treasury (including Lockbox, Electronic Development Applications vendor, Pay.gov, Remittance Express, Integrated Professional Automation Computer and Ca\$hLinkII)
- United States Postal Service (to obtain updated contact information).

DOED Perkins may be required to interface and share information with the following non-government entities:

- Educational institutions (to coordinate the management of the loan with the educational institution's financial aid office)
- Direct Loan servicers and other servicers (in connection with conversion/de-conversion of loans to/from the DOED Perkins system)
- Independent auditors (SSAE16, FSA auditors)
- National consumer reporting agencies (to obtain updated contact information and enrollment status)
- Person locator services (to obtain updated contact information)
- Other parties as authorized by the borrower (employers, references)
- NOCA (to obtain updated mailing address information)
- Optional support vendors (to provide services to the DOED Perkins system in connection with DOED Perkins servicing of DoED loans).

DOED Perkins does not share the information with any external entities except to process and service the borrower's loans and as permitted by the Privacy Act of 1974. The information is only shared as required to complete FSA's business related to the student loans. Information shared outside of the Department of Education is shared through secure encrypted transmissions and email.

Sharing of information with Federal government agencies will be pursuant to a Memorandum of Understanding (MOU) or Interconnection Security Agreement (ISA) and/or pursuant to other contractual or regulatory requirements. Sharing of information with certain other entities (consumer reporting agencies, independent program participants, etc.) will be pursuant to contractual or regulatory requirements or through sharing between the applicable entities and the Department of Education.



See response to question 4 hereof to review the risk to privacy from external sharing and disclosure and how the risks are mitigated.

Additionally:

- All information is protected by multi-factor authentication and monitored by automated and manual controls
- Data is housed within ECSI's secure data center facilities
- All data is encrypted or otherwise secured, as appropriate, as it moves between the DOED Perkins system and DoED systems, government systems, schools, guaranty agencies, lenders, servicer's, independent auditors, private collection agencies, national consumer reporting agencies, the United States Postal Service, person locator services, NCOA and any approved entity.

9. **Notice.** Is notice provided to the individual prior to collection of their information (e.g., a posted Privacy Notice)? What opportunities do individuals have to decline to provide information (where providing the information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

A privacy notice/policy is presented to the borrower via the following channels:

- Pursuant to the Gramm-Leach-Bliley Act, DoED's privacy notice is sent to the borrower by letter or email upon purchase of the loan by DoED and on an annual basis thereafter for the life of the loan
- A privacy notice is provided on the Free Application for Federal Student Aid (FAFSA) form and on the FAFSA online application website ([www.fafsa.ed.gov](http://www.fafsa.ed.gov))
- In order to establish an online account on the DOED Perkins system secure portal website, the borrower must agree to the Terms of Service, which incorporates the privacy policy by reference and link.

DOED Perkins will send a written Privacy Notice to borrowers, which is included in their Welcome Package, when they initially convert to the DOED Perkins system and annually thereafter.

The borrower has the opportunity to decline to provide information to the DOED Perkins system; however, providing certain information is required in order to (i) communicate with the DOED Perkins system through its secure borrower website or the DOED Perkins system's customer service call center, or (ii) receive certain benefits on a loan (such as deferment, forbearance, discharge, or forgiveness).

10. **Web Addresses.** List the web addresses (known or planned) that have a Privacy Notice.

[www.fafsa.ed.gov](http://www.fafsa.ed.gov)  
[www.efpls.com](http://www.efpls.com)  
[borrower.efpls.com](http://borrower.efpls.com)  
[client.efpls.com](http://client.efpls.com)

11. **Security.** What administrative, technical, and physical security safeguards are in place to protect the PII? Examples include: monitoring, auditing, authentication, firewalls, etc. Has a C&A been completed? Is the system compliant with any federal security requirements?



In accordance with the Federal Information Security Management Act of 2002 (FISMA), every FSA system must receive a signed Authority to Operate (ATO) from a designated FSA official. The ATO process includes a rigorous assessment of security controls, a plan of action and milestones (POAM) to remediate any identified deficiencies, and a continuous monitoring program. The DOED Perkins system received an ATO on August 1, 2013 and is compliant with all Federal Security requirements (OMB Circular A130, NIST 800-53 and FISMA).

FISMA controls implemented comprise a combination of management, operational and technical controls, and include the following control families.

The security safeguards in place include:

- Audit Trail
- Authentication Controls
- Signed Rules of Behavior
- Password Controls
- Access Privileges
- OMB Clearances
- Security Awareness Training
- Vulnerability Scanning
- Change Management Process
- Separation of duties
- Continuous Monitoring
- Annual Auditing
- System Firewalls
- Intrusion Detection Software
- Session Controls
- Encryption

12. **Privacy Act System of Records.** Is a system of records being created or altered under the Privacy Act, 5 U.S.C. 552a? Is this a Department-wide or Federal Government-wide SORN? If a SORN already exists, what is the SORN Number?

DOED Perkins is covered under the “Common Services for Borrowers” System of Records Notice (SORN), which was published as number 18-11-16 in the Federal Register on January 23, 2006 (71 FR 3503-3507).

13. **Records Retention and Disposition.** Is there a records retention and disposition schedule approved by the National Archives and Records Administration (NARA) for the records created by the system development lifecycle AND for the data collected? If yes – provide records schedule number:

Per FSA, DOED Perkins will follow the FSA “Loan Servicing, Consolidation and Collections Records” records schedule. These records are temporary. They will be cut-off annually upon payment or discharge of loan, and will be destroyed/deleted 15 years after cut off.