# 06.1 HHS Privacy Impact Assessment (Form) / NIH OD Loan Repayment Programs Website [System] (Item)

Primavera ProSight

Form Report, printed by: Hummel, Eric, **May 29, 2013**

## PIA SUMMARY

**1**

*The following required questions with an asterisk (*) represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget (OMB) and public posting in accordance with OMB Memorandum (M) 03-22.*

*Note: If a question or its response is not applicable, please answer "N/A" to that question where possible. If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of personally identifiable information (PII). If no PII is contained in the system, please answer questions in the PIA Summary Tab and then promote the PIA to the Senior Official for Privacy who will authorize the PIA. If this system contains PII, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.*

**2 Summary of PIA Required Questions**

**Is this a new PIA?*

No

*If this is an existing PIA, please provide a reason for revision:*

PIA Validation

**1. Date of this Submission:*

Sep 11, 2012

**2. OPDIV Name:*

NIH

**4. Privacy Act System of Records Notice (SORN) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):*

09-25-0165

**5. OMB Information Collection Approval Number:*

OMB No. 0925-0361

**6. Other Identifying Number(s):*

NIH/OER/DLR – LRP System6

**7. System Name (Align with system item name):*

National Institutes of Health (NIH) Division of Loan Repayment (DLR) - Loan Repayment Program (LRP) System

**9. System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:*

| **Point of Contact Information** | |
|---|---|
| **POC Name** | Steve Boehlert |

**10. Provide an overview of the system:*

The NIH Loan Repayment Programs (LRPs) are a vital component of our nation's efforts to attract health professionals to careers in clinical, pediatric, health disparity, or contraceptive and infertility research. In exchange for a two-year commitment to a research career, NIH will repay up to $35,000 per year of qualified educational debt, and covers Federal and state taxes that result from these benefits. The NIH LRP Website and Electronic Application System provides a web-based interface for individuals to obtain information, such as eligibility requirements and conditions for participating in the NIH loan repayment programs. The website also provides an electronic application system. Applicants log in to a secure website and provide all required documents, and can view the status of all forms they have submitted, as well as the status of forms submitted on their behalf by their supervisors, recommenders, and institutional officials. The NIH LRP system support the NIH strategic goal to foster highly skilled and diverse workforce focused on research goals. As this investment allows applicants to apply for loan repayment online and submit forms electronically, therefore it supports the E-Gov initiatives. The program manages and complies with the NIH Privacy Act System of Record # 09-25-0165, entitled "National Institutes of Health Office of Loan Repayment and Scholarship (OLRS) Records System, HHS/NIH/OD."

**13. Indicate if the system is new or an existing one being modified:*

Existing

**17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?*

*TIP: If the answer to Question 17 is "No" (indicating the system does not contain PII), only the remaining PIA Summary tab questions need to be completed and submitted. If the system does contain PII, the full PIA must be completed and submitted. (Although note that "Employee systems," – i.e., systems that collect PII "permitting the physical or online contacting of a specific individual … employed [by] the Federal Government – only need to complete the PIA Summary tab.)*

Yes

*17a. Is this a GSS PIA included for C&A purposes only, with no ownership of underlying application data? If the response to Q.17a is Yes, the response to Q.17 should be No and only the PIA Summary must be completed.*

**19. Are records on the system retrieved by 1 or more PII data elements?*

Yes

**21. Is the system subject to the Privacy Act? (If the response to Q.19 is Yes, the response to Q.21 must be Yes and a SORN number is required for Q.4)*

Yes

**23. If the system shares or discloses PII, please specify with whom and for what purpose(s):*

Sallie Mae, AES, Department of Education, to request loan accessing information and Institutional Officials and Non-NIH Scientists.

The LRP system interfaces with IMPAC II (Information for Management, Planning, Analysis and Coordination). IMPAC II is the successor to NIH's original IMPAC information management system. Its firewalls and user access controls ensure the security of confidential grant, contract, and personal data. NIH staff and authorized users from other U.S. Government agencies involved in health research have access to IMPAC II on a need-to-know basis.

The DLR LRP administers the application and disbursement processes for all of the LRPs, which includes information dissemination, conducting the application receipt and referral process, referring qualified applications to the NIH Institutes and Centers (ICs), evaluating educational debt, reviewing basic eligibility, administering individual LRP contracts, establishing repayment
The NIH LRP Website and Electronic Application System provides a web-based interface for individuals to obtain information, such as eligibility requirements and conditions for participating in the NIH loan repayment programs (LRPs). The website also provides an electronic application system. Applicants log in to a secure website and provide all required documents, and can view the status of all forms they have submitted, as well as the status of forms submitted on their behalf by their supervisors, recommenders, and institutional officials. The NIH DLR LRP system support the NIH strategic goal to foster highly skilled and diverse workforce focused on research goals. As this investment allows applicants to apply for loan repayment online and submit forms electronically, therefore it supports the E-Gov initiatives. The NIH System of Record # 09-25-0165, entitled "National Institutes of Health Office of Loan Repayment and Scholarship (OLRS) Records System, HHS/NIH/OD." NOTE: We have submitted an update to the SORN – to be renamed NIH Division of Loan Repayment (DLR) Records System

The LRP system interfaces with IMPAC II (Information for Management, Planning, Analysis and Coordination). IMPAC II is the successor to NIH's original IMPAC information management system. Its firewalls and user access controls ensure the security of confidential grant, contract, and personal data. NIH staff and authorized users from other U.S. Government agencies involved in health research have access to IMPAC II on a need-to-know basis.

The NIH DLR administers the application and disbursement processes for all of the LRPs, which includes information dissemination, conducting the application receipt and referral process, referring qualified applications to the NIH Institutes and Centers (ICs), evaluating educational debt, reviewing basic eligibility, administering individual LRP contracts, establishing repayment schedules with lending institutions, and obligating funds. Participating NIH ICs convene panels consisting of non-NIH scientists to review, score, and rank applications. The ICs make funding decisions and notify NIH DLR of the results of these decisions. Staff within the ICs coordinate with the NIH DLR to ensure funds are available and that they are charged to the appropriate CAN. These NIH staff also help guide applicants and participants who have questions about the research component of their applications or about other aspects of the application process, such as the peer review process.

The NIH DLR maintains and complies with the NIH Privacy Act System of Record # 09-25-0165, entitled "National Institutes of Health Office of Loan Repayment and Scholarship (OLRS) Records System, HHS/NIH/OD."

**30. Please describe in detail: (1) The information the agency will collect, maintain, or disseminate (clearly state if the information contained in the system ONLY represents federal contact data); (2) Why and for what purpose the agency will use the information; (3) Explicitly indicate whether the information contains PII; and (4) Whether submission of personal information is voluntary or mandatory:*

The information collected in the application forms is: name, social security number (SSN), grant number, program application and associated forms, service pay-back obligations, employment data, professional performance and credentialing history of licensed health professionals; personal, professional, and (voluntary) demographic background information; financial data including loan balances, deferment, forbearance, and repayment/delinq-uent/default status information; educational data including academic program; employment status and salary verification (which includes certifications and verifications of continuing participation in qualified research); credit reports; and Federal, State and county tax related information, including copies of tax returns.

LRP awards are competitive. The information collected during the LRP application process is used to make basic eligibility determinations

and to provide the scientific reviewers the information necessary to assess the potential of the applicant to pursue a career in research and to measure the quality of the overall environment to prepare the applicant for a research career.

Major changes are posted in the Federal Register and public comment is requested.

User consent is implicit in the act of providing the information. Providing the information is voluntary; however, in most circumstances failing to provide the information precludes the applicant from qualifying for the program or precludes the participant from receiving benefits of the program.

The information provided is not disclosed without the applicant/partic-ipant's consent to anyone outside of NIH in a manner that identifies the applicant/partic-ipant, except as permitted by the Privacy Act.

**31. Please describe in detail any processes in place to: (1) Notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of the original collection); (2) Notify and obtain consent from individuals regarding what PII is being collected from them; and (3) How the information will be used or shared. (Note: Please describe in what format individuals will be given notice of consent [e.g., written notice, electronic notice, etc.]):*

A copy of our Privacy Act Notification is posted on our Web site (http://www.lrp.nih.gov/privacy/index.htm ) and is available to all individuals providing IIF. The Privacy Act Notification lists the purposes for collecting the information, as well as the routine uses permitted by the Privacy Act. The system also informs the user when collecting data – during registration - "Note: We collect your Social Security Number [SSN] to verify your identity, to determine your eligibility for loan repayment assistance and to keep track of the federal funds you receive. We also use your SSN for loan repayment and servicing purposes under the Loan Repayment Program. We also use this information to determine whether you are eligible for loan repayment and the amount of that assistance. See Privacy Act information for additional information."

Major changes are posted in the Federal Register and public comment is requested.

User consent is implicit in the act of providing the information. Providing the information is voluntary; however, in most circumstances failing to provide the information precludes the applicant from qualifying for the program or precludes the participant from receiving benefits of the program.

The information provided is not disclosed without the applicant/partic-ipant's consent to anyone outside of HHS in a manner that identifies the applicant/partic-ipant, except as permitted by the Privacy Act.

**32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of PII)*

Yes

**37. Does the website have any information or pages directed at children under the age of thirteen?*

No

**50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN)*

Yes

**54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls:*

The DLR LRP system permits only authorized and authenticated user access. Additionally, there are Federal (NIST, FIPS, OMB, GAO, agency-level HHS/NIH guidelines and directives compliant) and industry-best practices security measures in place to ensure the system utilizes and ensures the effective use of security controls and authentication tools to protect privacy to the extent feasible. Access to the LRP system user's records is restricted to authorized users behind the NIH CIT firewall. Risk of unauthorized access is, therefore, considered low. The DLR LRP system is maintained in strict compliance with the NIH Privacy Act System of Record # 09-25-0165, entitled "National Institutes of Health Office of Loan Repayment and Scholarship (OLRS) Records System, HHS/NIH/OD."

Authorized user access to information is limited to authorized personnel in the performance of their duties. Authorized personnel include system managers and their staffs, financial, fiscal and records management personnel, legal personnel, computer personnel, and NIH contractors and subcontractors, all of whom are responsible for administering the NIH LRPs.

Physical safeguards: Rooms where records are stored are locked when not in use. During regular business hours, rooms are unlocked but all controlled by on-site personnel. Security guards perform random checks on the physical security of the storage locations after duty hours, including weekends and holidays.

Procedural and Technical Safeguards: A password is required to access the terminal and a data set name controls the release of data to only authorized users. All users of personal information in connection with the performance of their jobs protect information from public view and from unauthorized personnel entering an unsupervised office. Data on local area network computer files is accessed by keyword known only to authorized personnel. Codes by which automated files may be accessed are changed periodically. This procedure also includes deletion of access codes when employees or contractors leave. New employees and contractors are briefed and the security department is notified of all staff members and contractors authorized to be in secured areas during working and nonworking hours. Individuals remotely accessing the secured areas of the DLR Internet sites have separate accounts and passwords, and all data transmitted between the server and workstations is encrypted.

NIH requires the completion of a computer-based training (CBT) course entitled 'Computer Security and Awareness' for NIH staff and contractors. This CBT provides an overview of basic IT security practices and the awareness that knowing or willful disclosure of the sensitive information processed in the LRP system can result in criminal penalties associated with the Privacy Act, Computer Security Act, and other federal laws that apply. This CBT can be found at http://irtsectra-ining.nih.gov/. User access may be requested only by personnel authorized by the Executive Officer. Users are not permitted system access until the required system training prerequisites are completed and they demonstrate the competencies required to fulfill their work responsibilities-. Users are certified as having fulfilled the requirements by their Executive Officer or his or her appointed representative who requests access for the user.

It should also be noted that the DLR LRP system runs as a part of the NIH (CIT/OIT) infrastructure, which also supports policy enforcement to validate security requirements and privacy requirements are being satisfied. Incident handling guidelines are detailed in the Office of the Director (OD) standard operating procedures "OD/EO/OIT Standard Operating Procedures for Malicious Code Attacks, Intrusions, and Offensive Emails" (at http://oit.od.ni-h.go-v/pubs/SOP_-ISSO.pdf) and the NIH Incident Handling Guidelines (at http://irm.cit.n-ih.gov/security/-ih_guidelines.ht-ml) are consistent with guidance issued by HHS.

The NIH ISSO and Incident Response Team (IRT) (along with the Security Team Network Operations Team, Web Development Teams, Server Administrator Teams) help assure the security of NIH systems, data, and biomedical research information while maintaining connectivity and interoperability- throughout NIH. The IRT responds to computer security incidents, characterizes the nature and severity of incidents, and when appropriate, provides immediate diagnostic and corrective actions. When real or probable malicious activity is detected, the IRT acts quickly and effectively to prevent unauthorized access to NIH systems and networks and to minimize the impact of each incident. The IRT works to ensure that needed, up-to-date, accurate and complete intrusion detection and malicious code warnings can be disseminated throughout NIH and those vulnerabilities are remediate commensurate with risk. Intrusion incidents identified by the DLR system personnel are required to be reported to the NIH IRT. Audit logs are reviewed by appropriate staff to ensure that browsing of the database does not take place. NIH infrastructure that DLR uses support policy enforcement through scan testing and penetration testing to validate security requirements and privacy requirements are being satisfied. SARA Scans are proactive scans run by CIT to check all systems for vulnerabilities.- CIT sends the results of these scans to OD monthly. Possible Hacker Intrusion Incidents are usually reported by CIT's Intrusion Detection System, e.g., pre-attack probes, unauthorized access attempts, denial of service attempts, or vulnerabilities identified as a result of a SARA scan. This could also include notification by an outside source that they are being attacked from a NIH IP address.

These practices are in compliance with the standards of Chapter 45-13 of the HHS General Administration Manual, "Safeguarding Records Contained in Systems of Records," supplementary Chapter PHS 45-13, and the Department's Automated Information System Security Handbook.

## PIA REQUIRED INFORMATION

### 1 HHS Privacy Impact Assessment (PIA)

*The PIA determines if Personally Identifiable Information (PII) is contained within a system, what kind of PII, what is done with that information, and how that information is protected. Systems with PII are subject to an extensive list of requirements based on privacy laws, regulations, and guidance. The HHS Privacy Act Officer may be contacted for issues related to Freedom of Information Act (FOIA) and the Privacy Act. Respective Operating Division (OPDIV) Privacy Contacts may be contacted for issues related to the Privacy Act. The Office of the Chief Information Officer (OCIO) can be used as a resource for questions related to the administrative, technical, and physical controls of the system. Please note that answers to questions with an asterisk (*) will be submitted to the Office of Management and Budget (OMB) and made publicly available in accordance with OMB Memorandum (M) 03-22.*

*Note: If a question or its response is not applicable, please answer "N/A" to that question where possible.*

### 2 General Information

**Is this a new PIA?*

No

*If this is an existing PIA, please provide a reason for revision:*

PIA Validation

**1. Date of this Submission:*

Sep 11, 2012

**2. OPDIV Name:*

NIH

*3. Unique Project Identifier (UPI) Number for current fiscal year (Data is auto-populated from the System Inventory form, UPI table):*

009-25-01-06-01--4619-00-110-219

**4. Privacy Act System of Records Notice (SORN) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):*

09-25-0165

**5. OMB Information Collection Approval Number:*

OMB No. 0925-0361

*5a. OMB Collection Approval Number Expiration Date:*

Jun 30, 2014

**6. Other Identifying Number(s):*

NIH/OER/DLR – LRP System6

**7. System Name: (Align with system item name)*

National Institutes of Health (NIH) Division of Loan Repayment (DLR) - Loan Repayment Program (LRP) System

*8. System Location: (OPDIV or contractor office building, room, city, and state)*

| System Location: | |
|---|---|
| **OPDIV or contractor office building** | HHS/NIH/OD/OIR |
| **Room** | Room 2E30 |
| **City** | Bethesda |
| **State** | MD |

**9. System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:*

| Point of Contact Information | |
|---|---|
| **POC Name** | Steve Boehlert |

*The following information will not be made publicly available:*

| | |
|---|---|
| **POC Title** | Director of Operations |
| **POC Organization** | HHS/NIH/OD/OER/OEP/DLR |
| **POC Phone** | 301-451-4465 |
| **POC Email** | boehlers@od.nih.gov |

**10. Provide an overview of the system: (Note: The System Inventory form can provide additional information for child dependencies if the system is a GSS)*

The NIH Loan Repayment Programs (LRPs) are a vital component of our nation's efforts to attract health professionals to careers in clinical, pediatric, health disparity, or contraceptive and infertility research. In exchange for a two-year commitment to a research career, NIH will repay up to $35,000 per year of qualified educational debt, and covers Federal and state taxes that result from these benefits. The NIH LRP Website and Electronic Application System provides a web-based interface for individuals to obtain information, such as eligibility requirements and conditions for participating in the NIH loan repayment programs. The website also provides an electronic application system. Applicants log in to a secure website and provide all required documents, and can view the status of all forms they have submitted, as well as the status of forms submitted on their behalf by their supervisors, recommenders, and institutional officials. The NIH LRP system support the NIH strategic goal to foster highly skilled and diverse workforce focused on research goals. As this investment allows applicants to apply for loan repayment online and submit forms electronically, therefore it supports the E-Gov initiatives. The program manages and complies with the NIH Privacy Act System of Record # 09-25-0165, entitled "National Institutes of Health Office of Loan Repayment and Scholarship (OLRS) Records System, HHS/NIH/OD."

## SYSTEM CHARACTERIZATION AND DATA CATEGORIZATION

### 1 System Characterization and Data Configuration

*11. Does HHS own the system?*

Yes

*11a. If no, identify the system owner:*

Name: Steve Boehlert
Component: National Institutes of Health
Address:
Phone:
Email: BoehlerS@mail.nih.gov
FAX:

*12. Does HHS operate the system? (If the system is operated at a contractor site, the answer should be No)*

Yes

*12a. If no, identify the system operator:*

**13. Indicate if the system is new or an existing one being modified:*

Existing

*14. Identify the life-cycle phase of this system:*

Operations/Maintenance

*15. Have any of the following major changes occurred to the system since the PIA was last submitted?*

No

| Please indicate "Yes" or "No" for each category below: | Yes/No |
|---|---|
| **Conversions** | No |
| **Anonymous to Non-Anonymous** | No |
| **Significant System Management Changes** | No |
| **Significant Merging** | No |
| **New Public Access** | No |
| **Commercial Sources** | No |
| **New Interagency Uses** | No |
| **Internal Flow or Collection** | No |
| **Alteration in Character of Data** | No |

*16. Is the system a General Support System (GSS), Major Application (MA), Minor Application (child) or Minor Application (stand-alone)?*

Major Application

**17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?*

Yes

*TIP: If the answer to Question 17 is "No" (indicating the system does not contain PII), only the remaining PIA Summary tab questions need to be completed and submitted. If the system does contain PII, the full PIA must be completed and submitted. (Although note that "Employee systems," – i.e., systems that collect PII "permitting the physical or online contacting of a specific individual … employed [by] the Federal Government – only need to complete the PIA Summary tab.)*

*Please indicate "Yes" or "No" for each PII category. If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII.*

| Categories: | Yes/No |
|---|---|
| **Name (for purposes other than contacting federal** | Yes |

| | |
|---|---|
| **employees)** | |
| **Date of Birth** | Yes |
| **Social Security Number (SSN)** | Yes |
| **Photographic Identifiers** | No |
| **Driver's License** | No |
| **Biometric Identifiers** | No |
| **Mother's Maiden Name** | No |
| **Vehicle Identifiers** | No |
| **Personal Mailing Address** | Yes |
| **Personal Phone Numbers** | Yes |
| **Medical Records Numbers** | No |
| **Medical Notes** | No |
| **Financial Account Information** | Yes |
| **Certificates** | Yes |
| **Legal Documents** | No |
| **Device Identifiers** | No |
| **Web Uniform Resource Locator(s) (URL)** | No |
| **Personal Email Address** | Yes |
| **Education Records** | No |
| **Military Status** | No |
| **Employment Status** | Yes |
| **Foreign Activities** | No |
| **Other** | No |

*17a. Is this a GSS PIA included for C&A purposes only, with no ownership of underlying application data? If the response to Q.17a is Yes, the response to Q.17 should be No and only the PIA Summary must be completed.*

*18. Please indicate the categories of individuals about whom PII is collected, maintained, disseminated and/or passed through. Note: If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII. Please answer "Yes" or "No" to each of these choices (NA in other is not applicable).*

| Categories: | Yes/No |
|---|---|
| **Employees** | Yes |
| **Public Citizen** | Yes |
| **Patients** | No |
| **Business partners/contacts (Federal, state, local agencies)** | No |
| **Vendors/Suppliers/Contractors** | Yes |
| **Other** | No |

**19. Are records on the system retrieved by 1 or more PII data elements?*

Yes

*Please indicate "Yes" or "No" for each PII category. If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII.*

| Categories: | Yes/No |
|---|---|

| | |
|---|---|
| **Name (for purposes other than contacting federal employees)** | Yes |
| **Date of Birth** | No |
| **SSN** | No |
| **Photographic Identifiers** | No |
| **Driver's License** | No |
| **Biometric Identifiers** | No |
| **Mother's Maiden Name** | No |
| **Vehicle Identifiers** | No |
| **Personal Mailing Address** | No |
| **Personal Phone Numbers** | No |
| **Medical Records Numbers** | No |
| **Medical Notes** | No |
| **Financial Account Information** | No |
| **Certificates** | No |
| **Legal Documents** | No |
| **Device Identifiers** | No |
| **Web URLs** | No |
| **Personal Email Address** | Yes |
| **Education Records** | No |
| **Military Status** | No |
| **Employment Status** | No |
| **Foreign Activities** | No |
| **Other** | Loan Repayment Program (LRP) Account Tracking Number |

*20. Are 10 or more records containing PII maintained, stored or transmitted/passed through this system?*

Yes

**21. Is the system subject to the Privacy Act? (If the response to Q.19 is Yes, the response to Q.21 must be Yes and a SORN number is required for Q.4)*

Yes

*21a. If yes but a SORN has not been created, please provide an explanation.*

## INFORMATION SHARING PRACTICES

### 1 Information Sharing Practices

*22. Does the system share or disclose PII with other divisions within this agency, external agencies, or other people or organizations outside the agency?*

Yes

| Please indicate "Yes" or "No" for each category below: | Yes/No |
|---|---|
| **Name (for purposes other than contacting federal employees)** | Yes |
| **Date of Birth** | No |
| **SSN** | Yes |
| **Photographic Identifiers** | No |
| **Driver's License** | No |
| **Biometric Identifiers** | No |
| **Mother's Maiden Name** | No |
| **Vehicle Identifiers** | No |
| **Personal Mailing Address** | Yes |
| **Personal Phone Numbers** | Yes |
| **Medical Records Numbers** | No |
| **Medical Notes** | No |
| **Financial Account Information** | Yes |
| **Certificates** | Yes |
| **Legal Documents** | No |
| **Device Identifiers** | No |
| **Web URLs** | No |
| **Personal Email Address** | Yes |
| **Education Records** | Yes |
| **Military Status** | No |
| **Employment Status** | Yes |
| **Foreign Activities** | No |
| **Other** | No |

**23. If the system shares or discloses PII please specify with whom and for what purpose(s):*

Sallie Mae, AES, Department of Education, to request loan accessing information and Institutional Officials and Non-NIH Scientists.

The LRP system interfaces with IMPAC II (Information for Management, Planning, Analysis and Coordination). IMPAC II is the successor to NIH's original IMPAC information management system. Its firewalls and user access controls ensure the security of confidential grant, contract, and personal data. NIH staff and authorized users from other U.S. Government agencies involved in health research have access to IMPAC II on a need-to-know basis.

The DLR LRP administers the application and disbursement processes for all of the LRPs, which includes information dissemination, conducting the application receipt and referral process, referring qualified applications to the NIH Institutes and Centers (ICs), evaluating educational debt, reviewing basic eligibility, administering individual LRP contracts, establishing repayment
The NIH LRP Website and Electronic Application System provides a web-based interface for individuals to obtain information, such as eligibility requirements and conditions for participating in the NIH loan repayment programs (LRPs). The website also provides an electronic application system. Applicants log in to a secure website and provide all required documents, and can view the status of all forms they have submitted, as well as the status of forms submitted on their behalf by their supervisors, recommenders, and institutional officials. The NIH DLR LRP system support the NIH strategic goal to foster highly skilled and diverse workforce focused on research goals. As this investment allows applicants to apply for loan repayment online and submit forms electronically, therefore it supports the

E-Gov initiatives. The NIH System of Record # 09-25-0165, entitled "National Institutes of Health Office of Loan Repayment and Scholarship (OLRS) Records System, HHS/NIH/OD." NOTE: We have submitted an update to the SORN – to be renamed NIH Division of Loan Repayment (DLR) Records System

The LRP system interfaces with IMPAC II (Information for Management, Planning, Analysis and Coordination). IMPAC II is the successor to NIH's original IMPAC information management system. Its firewalls and user access controls ensure the security of confidential grant, contract, and personal data. NIH staff and authorized users from other U.S. Government agencies involved in health research have access to IMPAC II on a need-to-know basis.

The NIH DLR administers the application and disbursement processes for all of the LRPs, which includes information dissemination, conducting the application receipt and referral process, referring qualified applications to the NIH Institutes and Centers (ICs), evaluating educational debt, reviewing basic eligibility, administering individual LRP contracts, establishing repayment schedules with lending institutions, and obligating funds. Participating NIH ICs convene panels consisting of non-NIH scientists to review, score, and rank applications. The ICs make funding decisions and notify NIH DLR of the results of these decisions. Staff within the ICs coordinate with the NIH DLR to ensure funds are available and that they are charged to the appropriate CAN. These NIH staff also help guide applicants and participants who have questions about the research component of their applications or about other aspects of the application process, such as the peer review process.

The NIH DLR maintains and complies with the NIH Privacy Act System of Record # 09-25-0165, entitled "National Institutes of Health Office of Loan Repayment and Scholarship (OLRS) Records System, HHS/NIH/OD."

*24. If the PII in the system is matched against PII in one or more other computer systems, are computer data matching agreement(s) in place?*

No

*25. Is there a process in place to notify organizations or systems that are dependent upon the PII contained in this system when major changes occur (i.e., revisions to PII, or when the system is replaced)?*

Yes

*26. Are individuals notified how their PII is going to be used?*

Yes

*26a. If yes, please describe the process for allowing individuals to have a choice. If no, please provide an explanation.*

Major changes are posted in the Federal Register and public comment is requested. An update of this system of records was published in the Federal Register on September 26, 2002 (67 Fed. Reg. 60744)].

Providing the information is voluntary; however, in most circumstances failing to provide the information precludes the applicant from qualifying for the program.

*27. Is there a complaint process in place for individuals who believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate?*

Yes

*27a. If yes, please describe briefly the notification process. If no, please provide an explanation.*

Complaints are accepted by the systems manager for the System of Records of the Department of Health and Human Services (DHHS) numbered 09-25-0165, entitled "National Institutes of Health, Office of Loan Repayment and Scholarship (OLRS) Records System, HHS/NIH/OD."Note: We have submitted an update to the SORN – to be renamed NIH Division of Loan Repayment (DLR) Records System in Feb/March 2008

*28. Are there processes in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy?*

Yes

*28a. If yes, please describe briefly the review process. If no, please provide an explanation.*

All data is stored, archived, and designated in accordance with the System of Records of the Department of Health and Human Services (DHHS) numbered 09-25-0165, entitled "National Institutes of Health, Office of Loan Repayment and Scholarship (OLRS) Records System, HHS/NIH/OD."

*29. Are there rules of conduct in place for access to PII on the system?*

Yes

*Please indicate "Yes," "No," or "N/A" for each category. If yes, briefly state the purpose for each user to have access:*

| Users with access to PII | Yes/No/N/A | Purpose |
|---|---|---|
| **User** | No | Users can only access their own information |
| **Administrators** | Yes | Only designated authorized administrators have access to the system to generate and |

| | | |
|---|---|---|
| | | track loan repayment awards and system reports. All employees and contractors receive annual privacy act training, which is conducted by the Systems Manager or designee for the System of Records of the Department of Health and Human Services (DHHS) numbered 09-25-0165, entitled "National Institutes of Health Office of Loan Repayment and Scholarship (OLRS) Records System, HHS/NIH/OD." |
| **Developers** | Yes | Only designated authorized developers have access to the production system (and database) for system administration and updates/maintenance. The developers have a separate development and testing environment. All employees and contractors receive annual privacy act training, which is conducted by the Systems Manager or designee for the System of Records of the Department of Health and Human Services (DHHS) numbered 09-25-0165, entitled "National Institutes of Health Office of Loan Repayment and Scholarship (OLRS) Records System, HHS/NIH/OD." |
| **Contractors** | Yes | The LRP system is operated (Administered and Developed/Maintained) by government and contractor personnel. |
| **Other** | No | |

**30. Please describe in detail: (1) The information the agency will collect, maintain, or disseminate (clearly state if the information contained in the system ONLY represents federal contact data); (2) Why and for what purpose the agency will use the information; (3) Explicitly indicate whether the information contains PII; and (4) Whether submission of personal information is voluntary or mandatory:*

The information collected in the application forms is: name, social security number (SSN), grant number, program application and associated forms, service pay-back obligations, employment data, professional performance and credentialing history of licensed health professionals; personal, professional, and (voluntary) demographic background information; financial data including loan balances, deferment, forbearance, and repayment/delinq-uent/default status information; educational data including academic program; employment status and salary verification (which includes certifications and verifications of continuing participation in qualified research); credit reports; and Federal, State and county tax related information, including copies of tax returns.

LRP awards are competitive. The information collected during the LRP application process is used to make basic eligibility determinations and to provide the scientific reviewers the information necessary to assess the potential of the applicant to pursue a career in research and to measure the quality of the overall environment to prepare the applicant for a research career.

Major changes are posted in the Federal Register and public comment is requested.

User consent is implicit in the act of providing the information. Providing the information is voluntary; however, in most circumstances failing to provide the information precludes the applicant from qualifying for the program or precludes the participant from receiving benefits of the program.

The information provided is not disclosed without the applicant/partic-ipant's consent to anyone outside of NIH in a manner that identifies the applicant/partic-ipant, except as permitted by the Privacy Act.

**31. Please describe in detail any processes in place to: (1) Notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of the original collection); (2) Notify and obtain consent from individuals regarding what PII is being collected from them; and (3) How the information will be used or shared. (Note: Please describe in what format individuals will be given notice of consent [e.g., written notice, electronic notice, etc.])*

A copy of our Privacy Act Notification is posted on our Web site (http://www.lrp.nih.gov/privacy/index.htm ) and is available to all individuals providing IIF. The Privacy Act Notification lists the purposes for collecting the information, as well as the routine uses permitted by the Privacy Act. The system also informs the user when collecting data – during registration - "Note: We collect your Social Security Number [SSN] to verify your identity, to determine your eligibility for loan repayment assistance and to keep track of the federal funds you receive. We also use your SSN for loan repayment and servicing purposes under the Loan Repayment Program. We also use this information to determine whether you are eligible for loan repayment and the amount of that assistance. See Privacy Act information for additional information."

Major changes are posted in the Federal Register and public comment is requested.

User consent is implicit in the act of providing the information. Providing the information is voluntary; however, in most circumstances failing to provide the information precludes the applicant from qualifying for the program or precludes the participant from receiving benefits of the program.

The information provided is not disclosed without the applicant/partic-ipant's consent to anyone outside of HHS in a manner that identifies the applicant/partic-ipant, except as permitted by the Privacy Act.

## WEBSITE HOSTING PRACTICES

### 1 Website Hosting Practices

**32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of PII)*

Yes

| Please indicate "Yes" or "No" for each type of site below. If the system hosts both Internet and Intranet sites, indicate "Yes" for "Both" only. | Yes/ No | If the system hosts an Internet site, please enter the site URL. Do not enter any URL(s) for Intranet sites. |
|---|---|---|
| **Internet** | Yes | http://www.lrp.nih.gov |
| **Intranet** | No | |
| **Both** | No | |

*33. Does the system host a website that is accessible by the public and does not meet the exceptions listed in OMB M-03-22?*

*Note: OMB M-03-22 Attachment A, Section III, Subsection C requires agencies to post a privacy policy for websites that are accessible to the public, but provides three exceptions: (1) Websites containing information other than "government information" as defined in OMB Circular A-130; (2) Agency intranet websites that are accessible only by authorized government users (employees, contractors, consultants, fellows, grantees); and (3) National security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-Government Act.).*

Yes

*34. If the website does not meet one or more of the exceptions described in Q. 33 (i.e., response to Q. 33 is "Yes"), a website privacy policy statement (consistent with OMB M-03-22 and Title II and III of the E-Government Act) is required. Has a website privacy policy been posted?*

Yes

*35. If a website privacy policy is required (i.e., response to Q. 34 is "Yes"), is the privacy policy in machine-readable format, such as Platform for Privacy Preferences (P3P)?*

Yes

*35a. If no, please indicate when the website will be P3P compliant:*

N/A

*36. Does the website employ tracking technologies?*

Yes

| Please indicate "Yes", "No", or "N/A" for each type of cookie below: | Yes/No/N/A |
|---|---|
| **Web Bugs** | No |
| **Web Beacons** | No |
| **Session Cookies** | Yes |
| **Persistent Cookies** | No |
| **Other** | NO |

**37. Does the website have any information or pages directed at children under the age of thirteen?*

No

*37a. If yes, is there a unique privacy policy for the site, and does the unique privacy policy address the process for obtaining parental consent if any information is collected?*

N/A

*38. Does the website collect PII from individuals?*

Yes

| Please indicate “Yes” or “No” for each category below: | Yes/No |
|---|---|
| **Name (for purposes other than contacting federal employees)** | Yes |
| **Date of Birth** | Yes |
| **SSN** | Yes |
| **Photographic Identifiers** | No |
| **Driver's License** | No |
| **Biometric Identifiers** | No |
| **Mother's Maiden Name** | No |
| **Vehicle Identifiers** | No |
| **Personal Mailing Address** | Yes |
| **Personal Phone Numbers** | Yes |
| **Medical Records Numbers** | No |
| **Medical Notes** | No |
| **Financial Account Information** | Yes |
| **Certificates** | Yes |
| **Legal Documents** | Yes |
| **Device Identifiers** | No |
| **Web URLs** | No |
| **Personal Email Address** | Yes |
| **Education Records** | Yes |
| **Military Status** | No |
| **Employment Status** | Yes |
| **Foreign Activities** | No |
| **Other** | NO |

*39. Are rules of conduct in place for access to PII on the website?*

Yes

*40. Does the website contain links to sites external to HHS that owns and/or operates the system?*

No

*40a. If yes, note whether the system provides a disclaimer notice for users that follow external links to websites not owned or operated by HHS.*

N/A

## ADMINISTRATIVE CONTROLS

### 1 Administrative Controls

*Note: This PIA uses the terms "Administrative," "Technical" and "Physical" to refer to security control questions—terms that are used in several Federal laws when referencing security requirements.*

*41. Has the system been certified and accredited (C&A)?*

Yes

*41a. If yes, please indicate when the C&A was completed:*

Aug 30, 2009

*41b. If a system requires a C&A and no C&A was completed, is a C&A in progress?*

Yes

*42. Is there a system security plan for this system?*

Yes

*43. Is there a contingency (or backup) plan for the system?*

Yes

*44. Are files backed up regularly?*

Yes

*45. Are backup files stored offsite?*

Yes

*46. Are there user manuals for the system?*

Yes

*47. Have personnel (system owners, managers, operators, contractors and/or program managers) using the system been trained and made aware of their responsibilities for protecting the information being collected and maintained?*

Yes

*48. If contractors operate or use the system, do the contracts include clauses ensuring adherence to privacy provisions and practices?*

Yes

*49. Are methods in place to ensure least privilege (i.e., "need to know" and accountability)?*

Yes

*49a. If yes, please specify method(s):*

User accounts are granted rights to data on a need to know basis.

Personnel are required to sign an NIH non-disclosure agreement (NDA) before gaining access to the system. In addition, management personnel use security profiles for each position based on required levels of data access and periodically review security-level designations; they restrict access to sensitive information on a need-to-know basis.

Audit trails are employed to maintain data integrity and audit access. Data access is granted according to NIH System of Record # 09-25-0165, entitled "National Institutes of Health Office of Loan Repayment and Scholarship (OLRS) Records System, HHS/NIH/OD." An update of this system of records was published in the Federal Register on September 26, 2002 (67 Fed. Reg. 60744)].

**50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN):*

Yes

*50a. If yes, please provide some detail about these policies/practices:*

Retention and destruction of IFF is performed in accordance with NIH System of Record # 09-25-0165, entitled "National Institutes of Health Office of Loan Repayment and Scholarship (OLRS) Records System, HHS/NIH/OD." An update of this SOR was published in the Federal Register on February 8, 2002 (67 FR 6043). Records are retained and disposed of under the authority of the NIH Records Control Schedule contained in NIH Manual Chapter 1743, Appendix I, "Keeping and Destroying Records" (HHS Records Management Manual, Appendix B-361), item 2300-537-1. Participant case files are transferred to a Federal Records Center one year after closeout and destroyed five years later. Closeout is the process by which it is determined that all applicable administrative actions and disbursements of benefits have been completed by the DLR and service obligations have been completed by the participant. Applicant case files are destroyed three years after disapproval or withdrawal of their application. Appeal and litigation case files are destroyed six years after the calendar year in which the case is closed. Other copies of these files are destroyed two years after the calendar year in which the case is closed.

## TECHNICAL CONTROLS

### 1 Technical Controls

*51. Are technical controls in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system?*

Yes

| Please indicate "Yes" or "No" for each category below: | Yes/No |
|---|---|
| **User Identification** | Yes |
| **Passwords** | Yes |
| **Firewall** | Yes |
| **Virtual Private Network (VPN)** | Yes |
| **Encryption** | Yes |
| **Intrusion Detection System (IDS)** | Yes |
| **Common Access Cards (CAC)** | No |
| **Smart Cards** | No |
| **Biometrics** | No |
| **Public Key Infrastructure (PKI)** | No |

*52. Is there a process in place to monitor and respond to privacy and/or security incidents?*

Yes

*52a. If yes, please briefly describe the process:*

The Privacy Act Systems Manager is notified of any privacy act system breach.

## PHYSICAL ACCESS

### 1 Physical Access

*53. Are physical access controls in place?*

Yes

| Please indicate "Yes" or "No" for each category below: | Yes/No |
|---|---|
| **Guards** | Yes |
| **Identification Badges** | Yes |
| **Key Cards** | Yes |
| **Cipher Locks** | No |
| **Biometrics** | No |
| **Closed Circuit TV (CCTV)** | No |

**54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls:*

The DLR LRP system permits only authorized and authenticated user access. Additionally, there are Federal (NIST, FIPS, OMB, GAO, agency-level HHS/NIH guidelines and directives compliant) and industry-best practices security measures in place to ensure the system utilizes and ensures the effective use of security controls and authentication tools to protect privacy to the extent feasible. Access to the LRP system user's records is restricted to authorized users behind the NIH CIT firewall. Risk of unauthorized access is, therefore, considered low. The DLR LRP system is maintained in strict compliance with the NIH Privacy Act System of Record # 09-25-0165, entitled "National Institutes of Health Office of Loan Repayment and Scholarship (OLRS) Records System, HHS/NIH/OD."

Authorized user access to information is limited to authorized personnel in the performance of their duties. Authorized personnel include system managers and their staffs, financial, fiscal and records management personnel, legal personnel, computer personnel, and NIH contractors and subcontractors, all of whom are responsible for administering the NIH LRPs.

Physical safeguards: Rooms where records are stored are locked when not in use. During regular business hours, rooms are unlocked but all controlled by on-site personnel. Security guards perform random checks on the physical security of the storage locations after duty hours, including weekends and holidays.

Procedural and Technical Safeguards: A password is required to access the terminal and a data set name controls the release of data to only authorized users. All users of personal information in connection with the performance of their jobs protect information from public view and from unauthorized personnel entering an unsupervised office. Data on local area network computer files is accessed by keyword known only to authorized personnel. Codes by which automated files may be accessed are changed periodically. This procedure also includes deletion of access codes when employees or contractors leave. New employees and contractors are briefed and the security department is notified of all staff members and contractors authorized to be in secured areas during working and nonworking hours. Individuals remotely accessing the secured areas of the DLR Internet sites have separate accounts and passwords, and all data transmitted between the server and workstations is encrypted.

NIH requires the completion of a computer-based training (CBT) course entitled 'Computer Security and Awareness' for NIH staff and contractors. This CBT provides an overview of basic IT security practices and the awareness that knowing or willful disclosure of the sensitive information processed in the LRP system can result in criminal penalties associated with the Privacy Act, Computer Security Act, and other federal laws that apply. This CBT can be found at http://irtsectra-ining.nih.gov/. User access may be requested only by personnel authorized by the Executive Officer. Users are not permitted system access until the required system training prerequisites are completed and they demonstrate the competencies required to fulfill their work responsibilities-. Users are certified as having fulfilled the requirements by their Executive Officer or his or her appointed representative who requests access for the user.

It should also be noted that the DLR LRP system runs as a part of the NIH (CIT/OIT) infrastructure, which also supports policy enforcement to validate security requirements and privacy requirements are being satisfied. Incident handling guidelines are detailed in the Office of the Director (OD) standard operating procedures "OD/EO/OIT Standard Operating Procedures for Malicious Code Attacks, Intrusions, and Offensive Emails" (at http://oit.od.ni-h.go-v/pubs/SOP_-ISSO.pdf) and the NIH Incident Handling Guidelines (at http://irm.cit.n-ih.gov/security/-ih_guidelines.ht-ml) are consistent with guidance issued by HHS.

The NIH ISSO and Incident Response Team (IRT) (along with the Security Team Network Operations Team, Web Development Teams, Server Administrator Teams) help assure the security of NIH systems, data, and biomedical research information while maintaining connectivity and interoperability- throughout NIH. The IRT responds to computer security incidents, characterizes the nature and severity of incidents, and when appropriate, provides immediate diagnostic and corrective actions. When real or probable malicious activity is detected, the IRT acts quickly and effectively to prevent unauthorized access to NIH systems and networks and to minimize the impact of each incident. The IRT works to ensure that needed, up-to-date, accurate and complete intrusion detection and malicious code

warnings can be disseminated throughout NIH and those vulnerabilities are remediate commensurate with risk. Intrusion incidents identified by the DLR system personnel are required to be reported to the NIH IRT. Audit logs are reviewed by appropriate staff to ensure that browsing of the database does not take place. NIH infrastructure that DLR uses support policy enforcement through scan testing and penetration testing to validate security requirements and privacy requirements are being satisfied. SARA Scans are proactive scans run by CIT to check all systems for vulnerabilities.- CIT sends the results of these scans to OD monthly. Possible Hacker Intrusion Incidents are usually reported by CIT's Intrusion Detection System, e.g., pre-attack probes, unauthorized access attempts, denial of service attempts, or vulnerabilities identified as a result of a SARA scan. This could also include notification by an outside source that they are being attacked from a NIH IP address.

These practices are in compliance with the standards of Chapter 45-13 of the HHS General Administration Manual, "Safeguarding Records Contained in Systems of Records," supplementary Chapter PHS 45-13, and the Department's Automated Information System Security Handbook.

## APPROVAL/DEMOTION

| 1 | System Information |
|---|---|
| **System Name:** | National Institutes of Health (NIH) Division of Loan Repayment (DLR) - Loan Repayment Program (LRP) System |

| 2 | PIA Reviewer Approval/Promotion or Demotion |
|---|---|
| **Promotion/Demotion:** | Promote |
| **Comments:** | Antoine D. Jones |
| **Approval/Demotion Point of Contact:** | Steve Boehlert |
| **Date:** | Sep 11, 2012 |

| 3 | Senior Official for Privacy Approval/Promotion or Demotion |
|---|---|
| **Promotion/Demotion:** | Promote |
| **Comments:** | |

| 4 | OPDIV Senior Official for Privacy or Designee Approval |
|---|---|

**Please print the PIA and obtain the endorsement of the reviewing official below. Once the signature has been collected, retain a hard copy for the OPDIV's records. Submitting the PIA will indicate the reviewing official has endorsed it**

**This PIA has been reviewed and endorsed by the OPDIV Senior Official for Privacy or Designee (Name and Date):**

**Name:** _____ **Date:** _____

| | |
|---|---|
| **Name:** | Karen Plá |
| **Date:** | Sep 28, 2012 |

| 5 | Department Approval to Publish to the Web |
|---|---|
| **Approved for web publishing** | Yes |
| **Date Published:** | Sep 1, 2009 |
| **Publicly posted PIA URL or no PIA URL explanation:** | http://www.hhs.gov/pia/nih.html |

| PIA % COMPLETE |
|---|

| 1 | PIA Completion | |
|---|---|---|
| **PIA Percentage Complete:** | 100.00 | |
| **PIA Missing Fields:** | | |