Sav

Privacy Impact Assessment Form

v 1.47.4

Question	Answer
1 OPDIV:	NIH
2 PIA Unique Identifier:	P-9218201-570012
2a Name:	Electronic Research Administration
3 The subject of this PIA is which of the following?	○ General Support System (GSS) ● Major Application ○ Minor Application (stand-alone) ○ Minor Application (child) ○ Electronic Information Collection ○ Unknown
3 Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
3b Is this a FISMA-Reportable system?	● Yes ○ No
4 Does the system include a Website or online application available to and for the use of the general public?	○ Yes ● No
5 Identify the operator.	● Agency ○ Contract
6 Point of Contact (POC):	POC Title: eRA ISSO POC Name: Thomas Mason POC Organization: HHS/NIH/OD/OER/ORIS/eRA POC Email: Mason@mail.nih.gov POC Phone: 301-451-9048
7 Is this a new or existing system?	○ New ● Existing
8 Does the system have Security Authorization (SA)?	● Yes ○ No
8a Date of Security Authorization	Apr 30, 2017

Sav

9	Indicate the following reason(s) for updating this PIA. Choose from the following options.	☐ PIA Validation (PIA Refresh/Annual Review) ☐ Significant System Management Change ☐ Change Anonymous to Non-Character of Anonymous ☐ Alteration in Data ☐ New Public Access ☐ New Interagency Uses ☐ Internal Flow or Collection ☐ Conversion ☐ Commercial Sources
10	Describe in further detail any changes to the system that have occurred since the last PIA.	No changes have occurred that impact the PIA, however, the previous PIA inadvertently did not indicate that the last 4 digits of the SSN are collected and stored.
11	Describe the purpose of the system.	The Electronic Research Administration (eRA) provides critical Information Technology (IT) infrastructure to manage over $30 billion in research and non-research grants awarded annually by NIH and other grantor agencies in support of the collective mission of improving human health. Agencies supported include: Agency for Healthcare Research and Quality (AHRQ) Centers for Disease Control and Prevention (CDC) Food and Drug Administration (FDA) Substance Abuse and Mental Health Services Administration (SAMHSA) Veterans Administration (VA) eRA is recognized as an NIH Enterprise System and is a designated Center of Excellence by the U.S. Department of Health and Human Services (HHS). eRA is used as a grants management shared service provider by other federal agencies to manage their grants. The eRA system aligns with Grants.gov (the one-stop Web portal for finding and applying for federal grants), allowing for full electronic processing of grant applications from application submission through closeout of the grant award. The eRA program is a component of the NIH Office of Extramural Research (OER), headquartered in Bethesda, Maryland. Additional program information can be found at the eRA home page, following this link, https://era.nih.gov.

12	Describe the type of information the system will collect, maintain (store), or share. (Subsequent questions will identify if this information is PII and ask about the specific data elements.)	The type of information eRA collects, stores and shares include personally identifiable information (PII) such as: name, e-mail address, phone numbers, education information, mailing address, ethnicity, gender, race, and last four digits of SSN. eRA has implemented role-based access controls which limits administration and functional user privileges. Authentication (allowing users to log in to the system) is handled by NIH Login, which is administered by CIT's Identity and Access Management Team. NIH Login has its own approved PIA and Authority to Operate. NIH Login permits authentication to eRA via PIV Cards (for agency users) and username/password for external (grantee) users. Passwords are stored by NIH Login and subject to their PIA. Authorization (assigning roles and privileges to users) is handled within the eRA system, and the roles assigned to users are stored within the eRA database.

Sav

13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	eRA supports the full grants life cycle and is used by applicants and grantees worldwide. eRA maintains a variety of pre-award and award management records that contain information needed to process applications and manage grant awards across the award lifecycle. The type of information eRA collects, stores and shares include personally identifiable information (PII) such as: name, e-mail address, phone numbers, education information, mailing address, ethnicity, gender, race, and last four digits of SSN. Listed below are the categories of individuals, with pre-award and award management records collected about them: Applicants for or Awardees of awards - pre-award and award management (awardees) information; Individuals named in applications, , or awards - pre-award and award management (awardees) information; Referees - pre-award information; Peer Reviewers - pre-award information; Individuals required to report inventions, award management information; and Academic medical faculty, medical students and resident physicians - award management information. eRA has implemented role-based access controls which limits administration and functional user privileges. Authentication (allowing users to log in to the system) is handled by NIH Login, which is administered by CIT's Identity and Access Management Team. NIH Login has its own approved PIA and Authority to Operate. NIH Login permits authentication to eRA via PIV Cards (for agency users) and username/password for external (grantee) users. Passwords are stored by NIH Login and subject to their PIA. Authorization (assigning roles and privileges to users) is handled within the eRA system, and the roles assigned to users are stored within the eRA database.
14	Does the system collect, maintain, use or share **PII**?	Ye s No

Sav

15	Indicate the type of PII that the system will collect or maintain.	☐ Social Security Number ☐ Name ☐ Date of Birth ☐ Photographic Identifiers ☐ Driver's License Number ☐ Biometric Identifiers ☐ Mother's Maiden Name ☐ Vehicle Identifiers ☐ E-Mail Address ☐ Mailing Address ☐ Phone Numbers ☐ Medical Records Number ☐ Medical Notes ☐ Financial Account Info ☐ Certificates ☐ Legal Documents ☐ Education Records ☐ Device Identifiers ☐ Military Status ☐ Employment Status ☐ Foreign Activities ☐ Passport Number ☐ Taxpayer ID
16	Indicate the categories of individuals about whom PII is collected, maintained or shared.	☐ Employees ☐ Public ☐ Citizens ☐ Business Partners/Contacts (Federal, state, local agencies) ☐ Vendors/Suppliers/Contractors ☐ Patients ☐ Other
17	How many individuals' PII is in the system?	100,000-999,999

18	For what primary purpose is the PII used?	The primary purpose of Personally Identifiable Information (PII) entered into eRA modules is for NIH grant proposal submission and administration business processes. When a user account is established at the request of the individual, PII is requested about users in the roles of applicants, awardees of the institutional organization staff and or key personnel. Submission of PII is voluntary; however, in order to process a transaction, most fields are required. The records contained within this system will pertain to the following categories of individuals: Applicants for or Awardees of awards - pre-award and award management (awardees) information; Individuals named in applications, or awards - pre-award and award management (awardees) information; Referees - pre-award information; Peer Reviewers - pre-award information; Individuals required to report inventions, award management information; and, Academic medical faculty, medical students and resident physicians - award management information.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	As an NIH enterprise system and HHS Center of Excellence, eRA uses aggregate data (including some PII) for internal evaluation purposes: including trend analysis, budget and business forecasting.
20	Describe the function of the SSN.	Full Social Security Numbers are not used within the system. The last 4 digits of the SSN are used to assist in identifying and disambiguating individuals.
20a	Cite the **legal authority** to use the SSN.	Executive Order 9397

Sav

21	Identify **legal authorities** governing information use and disclosure specific to the system and program.	The legal authorities to operate and maintain this Privacy Act records system are: 5 U.S. Code §301- U.S. Government Organization and Employees - Departmental Regulations 42 U.S.C. §§ 217a- Public Health Service Act - Advisory councils or committees 42 U.S.C. §§ 241 - Public Health Service Act Research and Investigations 42 U.S.C. §§ 281 - Public Health Service Act , Organization of the National Institutes of Health 42 U.S.C. §§ 282 Public Health Service Act Director NIH, 42 U.S.C. §§ 284 Public Health Service Act , Directors of National Research Institutes 42 U.S.C. §§ 284a Public Health Service Act Advisory Councils, 42 U.S.C. §§ 288 Public Health Service Act Kirschstein National Research Service Awards 44 U.S.C. §§ 3101 Presidential Review of Records, Records Management by Agency Heads 35 U.S.C. § 200-212 Patent Rights in inventions made with Federal Assistance, 48 C.F.R. Subpart 15.3 Source Selection in competitive negotiated acquisitions and 37 C.F.R. 401.1-16 Bayh-Dole Act 44 U.S.C. Sec. 2904 General Responsibilities for Records Management 44 U.S.C. Sec. 2906 Inspection of Agency Records
22	Are records on the system retrieved by one or more PII data elements?	◉ Yes ○ No
22a	Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or identify if a SORN is being developed.	Published: SORN 09-25-0225 "NIH Electronic Research Administration (eRA) Records, HHS/NIH/OD/OER SORN 09-25-0036 "NIH Extramural Awards and Chartered Advisory Committee (IMPAC II), Contract Information (DCIS), and Cooperative Published: ☐ In Progress

Sav

23	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains ☐ In-Person ☐ Hard Copy: Mail/Fax Email Online ☐ Other Government Sources Within the OPDIV Other HHS OPDIV ☐ State/Local/Tribal ☐ Foreign Other Federal Entities ☐ Other Non-Government Sources Members of the Public ☐ Commercial Data Broker ☐ Public Media/Internet ☐ ◉ Private Sector Other
23 a	Identify the OMB information collection approval number and expiration date.	OMB # 0925-0001 Expiration Date:03/31/2020 OMB # 0925-0002 Expiration Date:03/31/2020
24	Is the PII shared with other organizations?	Yes ○ No

24a Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS

NIH Institutes and Centers (ICs) will have access for daily job duties supporting eRA award programs and related processes. Partnered agencies within HHS will have access to Personally Identifiable Information as well for the purpose of administering and facilitating joint grant and award programs.

Other Federal Agency/Agencies

For Agency partners using the eRA system, such as the Department of Defense (DoD) and Veterans Affairs (VA), access to PII will be for the purpose of administering and facilitating joint grant and award programs.

The Department of Justice (DoJ) or to a court or other adjudicative body when a potential violation of law has occurred, there is an ongoing litigation involving a participant of an eRA program, or an employee is being represented by the DoJ or participating agency.

State or Local Agency/Agencies

When there is a violation of a law, disclosure may be made to the appropriate authority for enforcing, investigating, or prosecuting the violation.

A record from this system may be disclosed for hiring or retention of an employee, the issuance or retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant or other benefit.

Private Sector

To a partnered research party for the purpose of participation in an eRA grant or award funded initiative. These parties are vetted by NIH and must abide by federal regulations, laws, and NIH mandated security, privacy, and records requirements.

To qualified experts not within the definition of agency employees as prescribed in agency regulations or policies to obtain their opinions on applications for grants, Cooperative Research and Development Agreements (CRADAs), inventions, or other awards as a part of the peer review process.

24b	Describe any agreements in place that authorizes the information sharing or disclosure (e.g. Computer Matching Agreement, Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	eRA has established documented formal Information Sharing Agreement (ISA) relationships with partnering organizations. Those ISAs are listed in the NIH System Authorization Tool (NSAT). eRA has ISAs with the following entities: Agency for Healthcare Research and Quality (AHRQ) Centers for Disease Control and Prevention (CDC) Food and Drug Administration (FDA) Grants.gov NIH Business System NIH Integrated Service Center Substance Abuse and Mental Health Services Administration (SAMHSA) Unified Financial Management System (UFMS) Veterans Administration (VA) eRA-DoD (USAMRMC-CDMRP) Interconnection eRA-and-Grants.gov Program Management Office Interconnection
24c	Describe the procedures for accounting for disclosures	All disclosures required by the Freedom of Information Act are logged by the Freedom of Information Act Office of the NIH Office of the Director. The log contains the following fields: name and address of requester, institution/organization, date requested, purpose of the request/the use of the information, release of PII (yes or no), if released the nature of the release (e.g. electronic, paper), name of recipient and address of recipient if different than the requester. Per language in the eRA Partner Agreements and Interconnection Security Agreements (ISAs), parties are required to report privacy breaches or suspected breaches to eRA within one (1) hour of detection. Disclosure of privacy information between systems is managed under routine use notices. In addition system logs maintain transaction information only (not the PII itself) as a record or accounting of each time it discloses information as part of routine use.
25	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.	Individuals are provided a privacy disclosure notice when accessing eRA modules. A privacy notice informs the individual that personal information will be collected.
26	Is the submission of PII by individuals voluntary or mandatory?	Voluntary Mandatory
27	Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to opt-out, provide a reason.	Individuals opt-out of collection of personally identifiable information by not registering with commons, initiating an object to the information collection, provide a awardee request. Demographic information account and allows a "do not wish to provide" option.
	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure	An altered System of Records Notice (SORN) will be

Sav

28	published and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained.	in the Federal Register to provide revision.	

29	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.	CONTESTING RECORD PROCEDURE (REDRESS): As described in the exemption clauses of SORN 09-25-0225 certain material will be exempt from amendment; however, consideration will be given to all amendment requests addressed to the System Manager. Individuals whose information is contained in the records can write to the System Manager, reasonably identify the record and specify the information being contested, state the corrective action sought and the reason(s) for requesting the correction, and provide supporting information. The right to contest records is limited to information that is factually inaccurate
3	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. If no processes are in place, explain why not.	PII is obtained from the subject individual. They have unlimited access to the system through the eRA "Commons" to update or correct the information or to change their decision regarding use of the information as part of aggregate data. eRA performs regression testing to ensure functionality with every release to ensure PII is not compromised. eRA has reduced the PII collected as data and for display on forms within Commons. The policy office clears data collection efforts via OMB annually. In addition, the integrity, availability, and relevancy of PII in eRA is maintained via: Daily and weekly backups. Real-Time Data replication to an offsite location certified by NIH Daily reviewed audit reports to determine if any unauthorized user(s) have accessed the system and/or database and if any system parameters have been modified without prior authorization on system and/or database Annual recertification of users via designated NIH Institute Center or Office Coordinator. Accounts identified as no longer required are

Sav

31	Identify who will have access to the PII in the system and the reason why they require access.	Users	External users (grantees) have access to PII they provided and will be able to update their PII only. Access to others' PII is restricted. Individuals may also
		Administrators	Administrators have access to the entire system to ensure they are operating efficiently; patching and other maintenance related activities
		Developers	Developers have access to PII to develop new features and functionality to ensure data integrity and quality.
		Contractors	Direct Contractors have access to PII to support users and to maintain system functionality.
		Others	Referees - pre-award information; Peer Reviewers - pre-award information; For examples, individuals who will
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access is strictly limited according to the principle of least privilege, which means giving a user only those privileges which are essential to that user's work.	
33	Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.	eRA has implemented role-based access controls which limits administration and functional user privileges. Role based access has been implemented across eRA. Privacy and Security controls to ensure proper protection of information by allowing users only access to the minimum amount of PII necessary to perform their job.	
34	Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.	The NIH Security Awareness Training course is used to satisfy this requirement. According to NIH policy, all personnel who use NIH applications must attend security awareness training every year. There are four categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, and Records Management).	
35	Describe training system users receive (above and beyond general security and privacy awareness training).	System users are provided guidance about proper usage of PII and privacy awareness. Users are also required to agree to the eRA Rules of Behavior and Data Access Agreements.	
36	Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes No	

Sav

37 Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	Item E-0001 (DAA-0443-2013-0004-0001) Official case files of construction, renovation, endowment and similar grants. Disposition: Temporary. Cut off annually following completion of final grant-related activity that represents closing of the case file (e.g., project period ended). Destroy 20 years after cut-off; Item E-0002 (DAA-0443-2013-0004-0002) Official case files of funded grants, unfunded grants, and award applications, appeals and litigation records. Disposition: Temporary. Cut off annually following completion of final grant-related activity that represents closing of the case file (e.g., end of project period, completed final peer review, litigation or appeal proceeding concluded). Destroy 10 years after cut-off; Item E-0003 (DAA-0443-2013-0004-0003) Animal welfare assurance files. Disposition: Temporary. Cut off annually following closing of the case file. Destroy 4 years after cut-off; and, Item E-0004 (DAA-0443-2013-0004-0004) Extramural program and grants management oversight records. Disposition: Temporary. Cut off annually. Destroy 3

Sav

38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative Safeguards: Controls to ensure proper protection of information and information technology systems include, but are not limited to, the completion of a: Security Assessment and Authorization (SA&A) package Privacy Impact Assessment (PIA) Mandatory annual NIH Information Security and Privacy Awareness training - or comparable specific in-kind training offered by participating agencies that has been reviewed and accepted by the NIH eRA Information Systems Security Officer (ISSO) The SA&A package consists of a: Security Categorization e-Authentication Risk Assessment System Security Plan Evidence of Security Control Testing Plan of Action and Milestones Contingency Plan Evidence of Contingency Plan Testing. When the design, development, or operation of a system of records on individuals is required to accomplish an agency function, the applicable Privacy Act Federal Acquisition Regulation (FAR) clauses are inserted in solicitations and contracts. Physical Safeguards: Controls to secure the data and protect paper and electronic records, buildings, and related infrastructure against threats associated with their physical environment include, but are not limited to, the use of the HHS Employee Persona Identity Verification (PIV) ID and/or badge number and NIH key cards, security guards, cipher locks, biometrics, and closed-circuit TV. Paper records are secured under conditions that require at least two locks to access, such as in locked file cabinets that are contained in locked offices or facilities. Electronic media are kept on secure servers or computer systems. Technical Safeguards: eRA data is encrypted in transit, in use, and at rest. Controls executed by the computer system are employed to minimize the possibility of unauthorized access, use, or dissemination of the data in the system. They include, but are not limited to user identification, password protection, firewalls, virtual private network, encryption, intrusion detection system, common access cards, smart cards, biometrics and public key infrastructure.

Sav

39 Identify the publicly-available URL: https://public.era.nih.gov/ commons https://iEdison.gov https://Edison.gov

Sav

40	Does the website have a posted privacy notice?	Yes / No
40a	Is the privacy policy available in a machine-readable format?	Yes / No
41	Does the website use web measurement and customization technology?	Yes / No
41a	Select the type of website measurement and customization technologies is in use and if it is used to collect PII. (Select all that apply)	Technologies: Web beacons — Collects PII? Yes / No; Web bugs — Yes / No; Session Cookies — Yes / No; Persistent Cookies — Yes / No; Other... N/A
42	Does the website have any information or pages directed at children under the age of thirteen?	Yes / No
43	Does the website contain links to non-federal government websites external to HHS?	Yes / No
43a	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	Yes / No
	General Comments	

OPDIV Senior Official for Privacy Signature	HHS Senior Agency Official for Privacy