Save

Privacy Impact Assessment Form

Status Revised | Form Number | Form Date 10/03/2019 | v 1.47.4

Question	Answer
1 OPDIV:	National Institutes of Health
2 PIA Unique Identifier:	TBD
2a Name:	NCI Office of Acquisitions System (OASYS)
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
3a Identify the Enterprise Performance Lifecycle Phase of the system.	Implementation
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 ○ Contractor
6 Point of Contact (POC):	POC Title: Business Owner POC Name: Teresa A. Baughman POC Organization: NCI - Office of Acquisitions POC Email: teresa.baughman@nih.gov POC Phone: 240-276-5397
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	09/07/2017

Save

9 Indicate the following reason(s) for updating this PIA. Choose from the following options.

- ☐ PIA Validation (PIA Refresh/Annual Review)
- ☐ Anonymous to Non-Anonymous
- ☐ New Public Access
- ☐ Uses Internal Flow or Collection
- ☐ Commercial Sources
- ☐ Significant System Management Change
- ☐ Alteration in Character of Data
- ☐ New Interagency Conversion

OA System (OASYS)/FFRDC Contract Administration System (FCAS) moving to CloudOne. Also Vendor Portal will be added and will be public-facing through Login.gov for OASYS Vendor Portal and iTrust for FCAS Vendor Portal as FCAS vendor users will have PIV cards and only access through NIH Network or NIH VPN.

10 Describe in further detail any changes to the system that have occurred since the last PIA.

Once Vendor Portal is live (estimated date February 2020), OASYS and FCAS applications will allow vendors (contractors) to access the site to submit documentation (e.g. revised proposals and quotes, final proposals and quotes, responses to task order requests for proposals (TORFPs), responses to Blanket Purchase Agreement (BPA) Call Requests, contract deliverables, invoices)), to ask questions in response to TORFPs, request contracting officer's authorizations, and to notify contracting officers of contractually-obligated information via a Vendor Portal. The vendor portals will have separate URLs to OASYS and FCAS and will then feed the data to the system thereby protecting government data.
Additionally, both the Vendor Portals and the existing OASYS and FCAS sites will be housed within CloudOne, NCI's managed private Amazon Web Services (AWS) application hosting solution. The Office of Acquisitions System (OASYS/ FCAS) is a Web based application. It utilizes data from the NIH data warehouse as well as information collected directly by OASYS to manage various aspects of the acquisition life-cycle.

Save

11 Describe the purpose of the system.	The OASYS and FCAS system was originally created to replace OA's SharePoint site that was used for routing and approval of post-award contract correspondence (e.g. invoices and deliverables) submitted by contractors during contract period of performance and for close-out. At a base level, the OASYS Contract Administration module provides OA the same routing process for approving/rejecting vendor correspondence while receiving recommendation from the Program Office. The goal from the point of design was to incorporate additional functionality found in other systems such as eContracts and Yellowtask. With the addition of Vendor Portal which will incorporate the functionality of Task Order Request For Proposal (TORFP)-EZ, the TORFP-EZ system will be retired. The overall goal for implementing the OASYS and FCAS system is to assist NCI OA with consolidating multiple systems used throughout the acquisition life-cycle and streamline the process of collaboration between the Office of Acquisitions and the Program Office. After the implementation of the Contract Administration module, the system's user interface (UI) was improved to include user feedback and provide a smooth transition for the upcoming modules to accomplish this goal. The system also includes modules for planning and solicitations as well as a document repository where file reviews can be done. OASYS and FCAS is a supplemental system that does not usurp the authority of the principle contracting system National Institutes of Health (NIH) Business System (NBS) PRISM. PRISM remains the system of record for contract awards. OASYS and FCAS do not usurp the authority of NBS Oracle Financial as the system of record for contract funding actions, invoice approval and payment processing.
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.)	OASYS utilizes data in two ways: 1 Acquisition and contract data is pulled from the NIH data warehouse (nVision), on a read-only basis, and displayed to
13 Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The Office of Acquisitions System (OASYS) is a Web based application. It utilizes data from the NIH data warehouse (nVision) as well as information collected directly by OASYS to
14 Does the system collect, maintain, use or share **PII**?	(•) Yes ( ) No

Save

15 Indicate the type of PII that the system will collect or maintain.

- [ ] Social Security Number
- [ ] Date of Birth
- [ ] Name
- [ ] 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
- DUNs Number/GSA Unique Identifier Other...
- Other...
- Other...
- Other...

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?

5,000-9,999

18 For what primary purpose is the PII used?

The PII information used by OASYS and FCAS is derived from existing systems at NIH. For example, we pull user name, email address and work phone from the NIH Employee Directory (NED). We pull vendor information directly from nVision. This information is ultimately used by OASYS and FCAS for access control, routing, and collaboration. While not typical, PII information could also exist within documents uploaded into the OASYS and FCAS system but such PII would not be indexed nor searchable.

When Vendor Portal is released, PII will be used to ensure that NCI is able to contact the appropriate representatives from awardees, offerors and bidders. Additionally, PII will be collected to establish the vendor profile so that vendor users that are authorized can have access to their specific firm's account and documentation within

19 Describe the secondary uses for which the PII will be used (e.g. testing, training or research)

None

Save

20 Describe the function of the SSN.	System does not collect, store, or process SSNs.	
20a Cite the **legal authority** to use the SSN.	Not applicable (see question 20)	
21 Identify **legal authorities** governing information use and disclosure specific to the system and program. 241(d), 281.	42 U.S.C.	
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: 09-25-0216 NIH Electronic Directory (NED) Published: 09-25-0118 Contracts: Professional Services Contractors Published: ☐ In Progress	
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	
23a Identify the OMB information collection approval number and expiration date.	In Progress	
24 Is the PII shared with other organizations?	◉ Yes ○ No	

Save

24a	Identify with whom the PII is shared or disclosed and for what purpose.	☐ Within HHS The OASYS FCAS data and file uploads shall be utilized by members of the National Cancer Institute and other Institutes under the Health and Human Services Umbrella with proper authorization. Access depends on the distribution of contracting responsibility across these entities. ☐ Other Federal Agency/Agencies ☐ State or Local Agency/Agencies ☐ Private Sector
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)).	Sharing access is provided directly within the system when authorized Government users are granted permission.
24c	Describe the procedures for accounting for disclosures	PII will be collected at time of initial Vendor Portal account registration, when the account information is updated, and when additional vendor users are added by vendor user administrator roles. OA will maintain a record of which NCI OA users have access to each Vendor Portal Account.
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.	OASYS/FCAS will inform individuals within the initial email invitation inviting the Vendor to register for a Vendor Portal account by including the following statement in the body of the email invitation. Additionally, the following statement will be included on the first page after the login screen. "Collection of this information is authorized by The Public Health Service Act, Section 411 (42 USC 285a). Rights of participants are protected by The Privacy Act of 1974. Participation is voluntary, however in order for NCI Office of Acquisitions (OA) to provide access to the Vendor Portal for use in uploading deliverables and invoices and responding to and submitting requests to NCI OA, Vendor Portal registration is required. The information collected will be kept private to the extent provided by law. Names and other identifiers will not appear in any report other than what is utilized by NCI OA and program staff for routine day-to-day contract administration. Information provided will be combined for all participants and reported as summaries. You are being contacted by email to complete this Vendor Portal Registration form and a voluntary survey so that NCI can provide your Vendor Firm with Vendor Portal access and improve the website. The information you provide will be included in a Privacy Act system of records, and will be used and may be disclosed for the purposes and routine uses described and published in the following System of Records Notices (SORN): 09-25-0216 Administration: NIH Electronic Discovery and 09-25-0118 Contracts: Professional Services Contractors https://www.hhs.gov/foia/privacy/sorns/nih- sorns.html."

Save

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 object to the information collection, provide a reason.	The PII data is sourced from existing DHHS/NIH systems (NED, nVision). Those systems own the responsibility for allowing users to opt out of providing certain information. OASYS and FCAS does not collect any new PII. Once the Vendor Portals are released, in order to obtain a vendor portal account, the vendor's business official is required to provide his or her name, title, their vendor email address, etc., as noted above. Vendor's are not required to respond to or bid on task orders. If they elect to respond to a request for proposal or revised proposal, they must provide required PII to establish the account for validation. This is to ensure that access is provided only to authorized vendor users, to facilitate proper routing and notification of subsequent award decisions, and to ensure that NCI users are able to contact awardees through the system post-award. The contractors must submit their deliverables, invoices, requests, notifications and other correspondence, through the vendor portal. Terms and conditions will be included in NCI OA awards mandating this.
28	Describe the process to notify and obtain consent previously 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 original collection). Alternatively, describe why they cannot be notified or have their consent obtained.	OASYS does not collect new PII, but uses PII shared under agreement with other NIH source systems mentioned. Once Vendor Portals are released, vendor's business officials will be contacted using the email and/or phone number information provided in their proposals/quotes and invited to submit revised proposals. Contractors with current contracts as of go live, will be given instructions by NCI OA, to establish a vendor portal profile for contract administration.
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.	OASYS does not collect PII, but uses shared PII under agreement with other NIH source systems. Those systems are responsible for resolving individuals' concerns over its use. However, if anyone feels their data has been inappropriately used as a result of OASYS and FCAS, then users can contact the OASYS and FCAS help desk. For Vendor Portals, the NCI OA will review its system logs and any other available historical information, and will work with the NCI Privacy Coordinator to investigate such concerns raised by vendor users.
30	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.	A PIA review will be conducted each time major OASYS and FCAS functionality is released that utilizes addition data (NED, nVision) beyond the data included in the previous PIA. Minimally, a PIA review will be conducted yearly.

Save

31 Identify who will have access to the PII in the system and the reason why they require access.	Users	Responsible for creating and managing requirements; Reviewing and dispositioning contract correspondence including OA and Program staff.
	Administrators	Responsible for Access control, Operations and Maintenance (O&M) support and in some cases the same responsibilities as "Users".
	Developers	Testing and customer defect resolution may expose these users to PII.
	Contractors	NCI contractor employees may be involved in the review correspondence process. Also, vendor users with vendor administrator roles would have access to their own firm's vendor profile.
	☐ Others	
32 Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Owner	All requests for access to OASYS and FCAS will be assigned an appropriate profile (role) and approved by the System before being implemented by the system administrator.
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.		Role based access controls are used to limit users' access to PII based on their defined job function and system role.
34 Identify training and awareness provided to NIH 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.	NIH	Each time the user initiates a new session, they are presented with a Terms of Use screen that will remind them of their responsibilities in protecting PII. All users are on the network have completed security, privacy, and management training. Additionally, all NCI staff and NCI contractors who will have access to the system or to the PII data complete the Security, Privacy, and Insider Threat course. This course is refreshed and all users must re-take each year.
35 Describe training system users receive (above and beyond general security and privacy awareness training).		All users are provided an opportunity to attend in-person OASYS and FCAS training sessions, and these sessions are scheduled on a regular basis. There are also training guides available directly through the applications.
36 Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?		◉ Yes ○ No
37 Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.		NIH Manual Chapter 1743, Appendix 1 allows records to be destroyed after a maximum period of six years and three months after final payment. Also, FAR 4.703(a)(b)(c)(d).

Save

38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	PII will not be exposed to users via business logic. PII data elements will be encrypted. Access to administrative features of the system will be controlled by ISSO and access permissions will be reviewed quarterly to ensure that users are aged out of the system. The system is operated inside the NCI Managed Data Center, within a dedicated federally leased building with armed guards, badge access, video surveillance; it is operated within the NCI's LAN GSS, which provides numerous technical security controls on behalf of its customers including firewalls, IDS/IPS, vulnerability scanners, centralized patching, host-based malware detection and prevention, and log aggregation and analyses.
	General Comments	
	OPDIV Senior Official for Privacy Signature	