1. OPDIV	National Institutes of Health
2. PIA Unique Identifier	P-7467403-400342
2a. Name	OD GSS: Certificates of Confidentiality
3. The subject of this PIA is which of the following?	Minor Application (child)
3a. Identify the Enterprise Performance Lifecycle Phase of the system.	Operational
3b. Is this a FISMA-Reportable system?	No
4. Does the system include a Website or online application available to and for the use of the general public?	Yes
Accept / Reject Status	Undefined
Question 4 Comment	
5. Identify the operator.	Agency
6. Point of Contact (POC)	
POC Title	System Owner
POC Name	Dawn Corbett
POC Organization	NIH/OD/OER/OEP
POC Email	dcorbett@mail.nih.gov
POC Phone	301.435.0921
Accept / Reject Status	Undefined
Question 6 Comment	
7. Is this a new or	New

existing system?	
8. Does the system have Security Authorization (SA)?	Yes
Accept / Reject Status	Undefined
Question 8 Comment	
8a. Date of Security Authorization	10/01/2017
9. Indicate the following reason(s) for updating this PIA. Choose from the following options.	
Other	
Accept / Reject Status	
Question 9 Comment	
10. Describe in further detail any changes to the system that have occurred since the last PIA.	
Accept / Reject Status	Undefined
Question 10 Comment	
11. Describe the purpose of the system.	Certificates of Confidentiality are issued by the National Institutes of Health (NIH) to protect the privacy of research subjects by protecting investigators and institutions from being compelled to release information that could be used to identify subjects associated with a research project. Certificates of Confidentiality are issued to institutions or universities

	where the research is conducted. They allow the investigator and others who have access to research records to refuse to disclose identifying information in any civil, criminal, administrative, legislative, or other proceeding, whether at the federal, state, or local level. Identifying information is broadly defined as any item or combination of items in the research data that could lead directly or indirectly to the identification of a research subject. By protecting researchers and institutions from being compelled to disclose information that would identify research participants, Certificates of Confidentiality help achieve the research objectives and promote participation in studies by assuring privacy to subjects.
Accept / Reject Status	Undefined
Question 11 Comment	
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.)	For a user to submit a Certificate of Confidentiality (CoC) application, the user will need to complete an application. The application requires users to provide the following information: E-mail address, name, organization, address, and phone number. Certificate of Confidentiality (CoC) also uses specific login information to assign permissions/user roles which is considered Personally Identifiable Information (PII). However, this is done by using the NIH Identity, Credential, and Access Management Services: Identity Management Services (IMS), formerly known as the Active Directory (AD), which combines the identity and authentication tools and capabilities used throughout the NIH enterprise. The IMS has its own approved PIA on record, including all legal authorities documented.
Accept / Reject Status	Undefined
Question 12 Comment	
13. Provide an overview of the system and describe the	Certificates of Confidentiality are issued by the National Institutes of Health (NIH) to protect the privacy of research subjects by protecting investigators

information it will collect, maintain (store), or share, either permanently or temporarily.	and institutions from being compelled to release information that could be used to identify subjects associated with a research project. Certificates of Confidentiality are issued to institutions or universities where the research is conducted. They allow the investigator and others who have access to research records to refuse to disclose identifying information in any civil, criminal, administrative, legislative, or other proceeding, whether at the federal, state, or local level. Identifying information is broadly defined as any item or combination of items in the research data that could lead directly or indirectly to the identification of a research subject. By protecting researchers and institutions from being compelled to disclose information that would identify research participants, Certificates of Confidentiality help achieve the research objectives and promote participation in studies by assuring privacy to subjects. For a user to submit a Certificate of Confidentiality (CoC) application, the user will need to complete an application. The application requires users to provide the following information: E-mail address, name, organization, address, and phone number. Certificate of Confidentiality (CoC) also uses specific login information to assign permissions/user roles which is considered Personally Identifiable Information (PII). However, this is done by using the NIH Identity, Credential, and Access Management Services: Identity Management Services (IMS), formerly known as the Active Directory (AD), which combines the identity and authentication tools and capabilities used throughout the NIH enterprise. The IMS has its own approved PIA on record, including all legal authorities documented.
Accept / Reject Status	Undefined
Question 13 Comment	
14. Does the system collect, maintain, use or share PII?	Yes

Accept / Reject Status	Undefined
Question 14 Comment	
15. Indicate the type of PII that the system will collect or maintain.	Name, E-Mail Address, Phone Numbers, Mailing Address
	affiliated organization
Accept / Reject Status	Undefined
Question 15 Comment	
16. Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees, Public Citizens
Accept / Reject Status	Undefined
Question 16 Comment	
17. How many individuals' PII is in the system?	50,000-99,999
Accept / Reject Status	Undefined
Question 17 Comment	
18. For what primary purpose is the PII used?	These records are used to: Identify applicants who have applied for CoC and issued one, and to assist NIH officials in maintaining the electronic record of the certificates issues and aid/help them during renewal.

Accept / Reject Status	Undefined
Question 18 Comment	
19. Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	N/A
Accept / Reject Status	Undefined
Question 19 Comment	
20. Describe the function of the SSN.	N/A
Accept / Reject Status	Undefined
Question 20 Comment	
20a. Cite the legal authority to use the SSN.	N/A
21. Identify legal authorities governing information use and disclosure specific to the system and program.	Section 301(d) of the Public Health Service Act as amended by Section 2012 of the 21st Century Cures Act allows NIH to issue, upon application, a Certificate of Confidentiality to institutions conducting non-NIH funded research. The COC application collects information to allow processing of these applications.
22. Are records on the system retrieved by one or more PII data elements?	Yes
Accept / Reject Status	Undefined
Question 22 Comment	

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:	09-25-0225 "NIH Electronic Research Administration (eRA) Records, HHS/NIH/OD/OER
Published:	
Published:	
In Progress	Undefined
23. Identify the sources of PII in the system.	Online, Within the OPDIV, Other HHS OPDIV, Members of the Public, Private Sector
Accept / Reject Status	Undefined
Question 23 Comment	
23a. Identify the OMB information collection approval number and expiration date.	O0925-0689, Expiration Date: 12/31/2019
24. Is the PII shared with other organizations?	No
Accept / Reject Status	Undefined
Question 24 Comment	
24a. Identify with whom the PII is shared or disclosed and for what purpose.	
Within HHS	
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)).	
24c. Describe the procedures for accounting for disclosures.	
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.	PII is a required submission of the application by the users. A link to the standard HHS and NIH/Office of the Director (OD)/Office of Extramural Research (OER) Privacy information is provided on the application form. If users do not want to provide their user credentials, they are unable to submit a CoC Application.
Accept / Reject Status	Undefined
Question 25 Comment	
26. Is the submission of PII by individuals voluntary or mandatory?	Voluntary
Accept / Reject Status	Undefined
Question 26 Comment	
27. Describe the method for individuals	Submission of a request for a Certificate of Confidentiality for non-NIH research is voluntary. As

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 statute allows NIH to issue institutions and investigators and specifies responsibilities of those investigators, collection of the name and contact information of these investigators is necessary. If an applicant does not want to disclose specific information (e.g. phone number), the applicant can contact the COC Coordinator to request bypassing a required field, if the application can reasonably be processed without this information.
Accept / Reject Status	Undefined
Question 27 Comment	
28. 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 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.	Current system users/administrators are given notice via e-mail when major system changes occur. We have not had any major changes to the system and do not disclose user data to non-NIH users. Users may be notified via email if such changes or disclosure may occur. Users establish an account using NIH sign-on and are notified of the following: By using this system, you understand and consent to the following: The Government may monitor, record, and audit your system usage, including usage of personal devices and email systems for official duties or to conduct HHS business. Therefore, you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this system. At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this system. Any communication or data transiting or stored on this system may be disclosed or used for any lawful Government purpose.
Accept / Reject Status	Undefined
Question 28 Comment	

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.	Individuals who believe their Personally Identifiable Information (PII) has been inappropriately obtained, used, or disclosed, or that it is inaccurate may contact the CoC Office NIH-CoC-Coordinator@mail.nih.gov for assistance. The COC Coordinator will determine the appropriate action such as deleting or correcting user data or consulting with the NIH Privacy Office and/or appropriate authorities as necessary.
Accept / Reject Status	Undefined
Question 29 Comment	
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.	Currently, there are no system specific processes for periodic review of PII. The COC Coordinator reviews the information for accuracy while conducting their assessment of the application. Information is corrected at the request of the applicant.
Accept / Reject Status	Undefined
Question 30 Comment	
31. Identify who will have access to the PII in the system and the reason why they require access.	
Users	Yes
	Access is required for submitting an application and verifying the status. Users have access only to PII for the applications they submit.
Administrators	Yes
	Access is required for administering the application and notifying users of the status of their COC, resolving any issues, and issuing a Certificate with accurate information.

Developers	Yes
	Access is required for development of the application and notifying users of system issues.
Contractors	Yes
	To support and troubleshoot the system. NIH uses direct contractors in various roles. Authorization to use the system is required and access is limited to those who need access to perform their role.
Others	No
32. Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access to the system is requested by CoC Business Owner. An email is submitted to NIH-COC-Help@od.nih.gov. An authorized Development Staff / Administrator routes the request to the NIH CoC Business Owner who in turn, provides permission to proceed with verification and approval. The NIH CoC Business owner approves access based on role based access controls and least privilege. Users will be granted access if they have a need to process COC requests, verify COC records, or contact COC applicants with information about their application. These roles require access to PIII. All employees and contractor who maintain the system sign non- disclosures at the time of onboarding. Disclosure of information to other Federal agencies are made in accordance with federal laws and regulations as described in the System of Records Notice (SORN) , as well as internal procedures.
Accept / Reject Status	Undefined
Question 32 Comment	
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.	Determinations are made based on Role based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job. As PII in the system is limited to applicant names and contact information, all users involved in processing COCs, verifying COC records, or contacting COC users require access to PII.
Accept / Reject Status	Undefined

Question 33 Comment	
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). Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.
Accept / Reject Status	Undefined
Question 34 Comment	
35. Describe training system users receive (above and beyond general security and privacy awareness training).	Users of the COC system receive training on system use as appropriate to their role. Users are expected to review the COC user manual for instructions on system use.
Accept / Reject Status	Undefined
Question 35 Comment	
36. Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
Accept / Reject Status	Undefined

Question 36 Comment	
37. Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	Records are retained in accordance with the NIH Administrative and Program Records Schedule 300-1.1a (Disposition Authority: DAA-0443-2017-0001), Certificates of Confidentiality issued for Intramural Research - Certificate of Confidentiality Support Documentation; and are cut off annually at expiration of the Certificate of Confidentiality. They are destroyed 6 years after the cutoff.
Accept / Reject Status	Undefined
Question 37 Comment	
38. Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Admin Safeguards: NIH staff, including direct contractors take mandatory security and privacy training and include system security and contingency plan. Access is via least privilege through role-based access, and policies for retention and destruction of PII are in place. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job. Files are backed up regularly and stored offsite. Contract clauses ensure adherence to privacy provisions and practices. Technical Controls: Access to the system is controlled by NIH log-in which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, organizational unit, and status of the report. All servers have been configured to remove all unused applications and system files and all local account access except when necessary to manage the system and maintain integrity of data. Physical Controls: The servers reside in the Office of Information Technology Data Center where policies and procedures are in place to restrict access to the machines. This includes guards at the front door and entrance to the machine room.
Accept / Reject Status	Undefined

Question 38 Comment	
39. Identify the publicly-available URL.	https://coc.od.nih.gov/
Accept / Reject Status	Undefined
Question 39 Comment	
40. Does the website have a posted privacy notice?	Yes
Accept / Reject Status	Undefined
Question 40 Comment	
40a. Is the privacy policy available in a machine-readable format?	Yes
41. Does the website use web measurement and customization technology?	No
Accept / Reject Status	Undefined
Question 41 Comment	
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).	
Web Beacons	
Collects PII?	

Web Bugs	
Collects PII?	
Session Cookies	
Collects PII?	
Persistent Cookies	
Collects PII?	
Other ...	
Collects PII?	
42. Does the website have any information or pages directed at children under the age of thirteen?	No
Accept / Reject Status	Undefined
Question 42 Comment	
42a. Is there a unique privacy policy for the website, and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
43. Does the website contain links to non-federal government websites external to HHS?	No
Accept / Reject Status	Undefined
Question 43 Comment	

43a. Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
REVIEWER QUESTIONS: The following section contains Reviewer Questions which are not to be filled out unless the user is an OPDIV Senior Officer for Privacy.	
1. Are the questions on the PIA answered correctly, accurately, and completely?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 1 Comment	
2. Does the PIA appropriately communicate the purpose of PII in the system and is the purpose justified by appropriate legal authorities?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 2 Comment	
3. Do system owners demonstrate appropriate understanding of the	Undefined

impact of the PII in the system and provide sufficient oversight to employees and contractors?	
Reviewer Notes	
Accept / Reject Status	Undefined
Question 3 Comment	
4. Does the PIA appropriately describe the PII quality and integrity of the data?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 4 Comment	
5. Is this a candidate for PII minimization?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 5 Comment	
6. Does the PIA accurately identify data retention procedures and records retention schedules?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 6 Comment	

7. Are the individuals whose PII is in the system provided appropriate participation?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 7 Comment	
8. Does the PIA raise any concerns about the security of the PII?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Accept / Reject Status	Undefined
Question 8 Comment	
9. Is applicability of the Privacy Act captured correctly and is a SORN published or does it need to be?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Accept / Reject Status	Undefined
Question 9 Comment	
10. Is the PII appropriately limited for use internally and with third parties?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined

Question 10 Comment	
11. Does the PIA demonstrate compliance with all Web privacy requirements?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 11 Comment	
12. Were any changes made to the system because of the completion of this PIA?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 12 Comment	
General Comments	This component is under the OD GSS, whose Universal Unique Identifier (UUID) is: : 2092B382-A4F2-4FD5-A93E-1857E18B771E.
Status and Approvals	
IC Status	IC Approved
OSOP Status	HHS Approved
OPDIV Senior Official for Privacy Signature	
HHS Senior Agency Official for Privacy	