Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	Identity, Credential, and Access Management (ICAM)		
Component:	U.S. Citizenship and Immigration Services (USCIS)	**Office or Program:**	OCIO
Xacta FISMA Name (if applicable):	Identity, Credential, and Access Management (ICAM)	**Xacta FISMA Number (if applicable):**	CIS-07028-GSS-08028
Type of Project or Program:	IT System	**Project or program status:**	Operational
Date first developed:	September 1, 2013	**Pilot launch date:**	N/A
Date of last PTA update	May 25, 2016	**Pilot end date:**	N/A
ATO Status (if applicable)	Complete	**ATO expiration date (if applicable):**	N/A

PROJECT OR PROGRAM MANAGER

Name:	Eduardo J. Lopez		
Office:	USCIS OIT	**Title:**	ICAM Program Chief
Phone:	**202-272-9858**	**Email:**	Eduardo.J.Lopez@uscis.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	Almena (Joi) Robbins		
Phone:	301-758-1626	**Email:**	Almena.J.Robbins@uscis.dhs.gov

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Updated PTA

This PTA is being updated to include (1) the option of a third-party application option for the two-factor authentication process and use of a backup code (ELIS only); (2) additional systems supported by ICAM; and (3) update general background consistent with current operations.

The USCIS Office of Information Technology (OIT) complies with mandates pertaining to the Federal Identity, Credential, and Access Management (FICAM) program. USCIS Identity, Credential, and Access Management (ICAM) is an enterprise-wide program that collectively manages identity, credential, access and federation, and provides the integrity for internal and USCIS users. It also provides external users access to USCIS systems.

How ICAM works for internal users (USCIS staff and partner agencies):

- Internal ICAM Users: This includes but is not limited to USCIS employees and contract staff as well as other individuals at DHS components, and partnering agencies (e.g., DOS, DOJ, DOL, etc.) who require access to USCIS systems.
- Collection of Information: ICAM data originates from USCIS Active Directory. The USCIS Network Account feeds information into ICAM.
- Use of Information: The information is used to provide authentication and authorization to access USCIS applications and systems supported by ICAM.
- Maintenance of Information: ICAM connects to ICAM LDAP and Active Directory. Active Directory automatically updates LDAP.

Internal USCIS applications and systems currently support by ICAM can be found in the Appendix.

How Public ICAM works for external users (USCIS customers):

- Public ICAM Users: This includes individual seeking immigration benefits or services provided by USCIS. These users may be applicants, beneficiaries, legal representatives or requestors.
- Collection of Information: Customers create accounts using email address. ICAM stores answers to challenge questions to facilitate password reset. In addition, authentication services require the individual to provide an email address and or SMS number; or opt for the use of a third-party authenticator application. This application is a new feature described below. ICAM generates a Universal Unique Identifier (UUID) for each account at time of creation, as well as the new feature to include a QR code or key to be used for application and back-up code. Information is collected in multiple-choice radio button format, and includes a "none of the above" option where appropriate.
- Use of Information: Information collected by ICAM is used to provide authentication and authorization to access USCIS applications housed within USCIS information systems.
- Maintenance of Information: Length of retention of records is dependent on the requirements of the systems that ICAM supports.
- UPDATE – External-facing applications and systems that currently leverage ICAM are USCIS ELIS, myUSCIS and myE-Verify.

Public ICAM-IDPaaS

Public ICAM also has the subsystem Identity Proofing as a Service (IDPaaS). This subsystem is designed to verify the identity of external users (customers) in order to ascertain who they are and provide them access to their intended USCIS system. IDPaaS is designed to verify that the customer requesting access to a USCIS system is who they say they are. IDPaaS uses information already provided by the customer to confirm the customer is the same. It is important to note that IDPaaS is a support system to other applications. IDPaaS is used to support identity verification of customers accessing the USCIS ELIS system only.

IDPaaS is a service that currently provides verifiable identity for customers interacting with USCIS Electronic Immigration System (USCIS ELIS). USCIS does not have a method to identity-proof individuals who have not lived or conducted business in the United States, which is a large portion of USCIS customers. This system presents a challenge-response for which the USCIS online account holder should know the answers. With this, USCIS can be assured that the customer is in fact the customer they say they are. IDPaaS generates questions and answers to the customer. Upon the customer providing answers, IDPaaS issues ICAM a Pass/Fail determination on whether the customer will be granted access to proceed. IDPaaS verifies information against a customer's Alien number and Department of State Case ID number to query legacy systems and create the question list. Once the customer passes the identity proofing quiz, USCIS ELIS retains the fact that the customer has been identity-proofed, and does not require the customer to repeat the process for subsequent immigration benefit requests.

UPDATE: *Public ICAM-Authentication Services:*

Public ICAM will allow users to use an third-party authenticator application (e.g., Google Authenticator, Authy, Microsoft Authenticator, etc.) to provide two-factor authentication (2FA) into their USCIS online account. This is how the authenticator application will be used:

- As part of the initial account creation, the user will have two options: the authenticator application OR an email address and SMS.
- The external user must either scan a QR code or enter a unique token manually generated by ICAM to pair the USCIS account with the specific authenticator application.
- The authenticator will then generate temporary one-time passwords which expire every 30 seconds. The temporary one-time password displayed on the user's mobile device must be entered into the ICAM system as a second level of authenticaton upon login.

This is a one time event that is presented to the user during account creation. Users may still continue to utilize either email or SMS delivery of their 2FA code. The selection and use of a third-party application is at the discretion of the end user. The use of 2FA (email, SMS, or authenticator application) provides validation that the user is in possession of the same mechanism used to create the account. The authenticator will receive from USCIS ICAM the user's email address and the shared secret key. The user has the ability to reset account 2FA preferences. FAQ for online account creation will be updated to reflect this change.

A Privacy Act Statement will be provided to notify the customer they should familiarize themself with the privacy policy of the third party application they choose since in some instances this will be the first contact with the company.

Typically, a user installs an Authenticator app on a mobile device. To log into a site or service that uses two-factor authentication, the user provides user name (email address) and password to the site and runs the Authenticator app. The app displays an additional six-digit one-time password and transmits it to the site, which asks the user what that password is. The user enters it, thus authenticating the user's identity.

UPDATE: *Public ICAM-Backup Code*:

The Public ICAM application presents users with a Backup Code, which users will be recommended to save or print, and utilize in the event they lose the authenticator app after changing mobile device or losing their mobile device. The back up code is a one-time use code that can be used to reset the user's account, 2FA preferences, and security questions and allows the user into the account after re-setting it back up under the same process as original account setup. After one-time use and new preferences set, a new code is provided to the user. Available to all users regardless of their preference. It resets their account then resets 2FA preference and security questions. The old backup code is no longer valid.

2. Does this system employ any of the following technologies: *If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.*	☐ Closed Circuit Television (CCTV) ☐ Social Media ☐ Web portal[1] (e.g., SharePoint) ☐ Contact Lists ☒ None of these

3. From whom does the Project or Program collect, maintain, use, or disseminate information? *Please check all that apply.*	☐ This program does not collect any personally identifiable information[2] ☒ Members of the public ☒ DHS employees/contractors (list components): USCIS ☒ Contractors working on behalf of DHS ☐ Employees of other federal agencies

4. What specific information about individuals is collected, generated or retained?

Updated Information

Public ICAM

- Email address

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

- Password
- Answers to challenge questions
- ICAM generates a UUID
- ICAM generates a QR code or key for authentication purposes
- Will store email and/or SMS number, or authenticator application as a two-factor authentication method. Bound by email address and not identity.

Internal ICAM

OMB MAX
First Name
Last Name
Email Address (confirmed via MAX registration)
PIV-UPN (parsed from the PIV Public Certificate)
Govt Agency/Department/Component (via the PIV-UPN)
LOA (via SAML Authn Context of https://max.gov/icam/2015/10/securityLevels/piv)

DHS AppAuth
First Name
Last Name
Email Address
PIV-UPN
uid (sAMAccountName)
AD domain
DHS Component (derived via the PIV-UPN)

CIS1 AD (synch)
District
Site
Region
Display Name
Employee Type (CIV, CTR, FSN)
First Name
Initials
Telephone Number
uid (sAMAccountName)
Email Address
CN
User Principal Name (PIV-UPN)
Location
Description
Manager
Last Name
SMARTCARD_REQUIRED
User Status (Active, Inactive, Deleted)

Membership in the EPMS_LOCAL group
AD domain (CIS1)
DHS Component (USCIS)

myAccess
PICSID
Application roles and attributes
Application role and attribute request/approval history
Membership in approval groups

IDPaaS

IDPaaS has two data sources, PCQS and USCIS ELIS. IDPaaS stores USCIS ELIS TOKEN, ICAM UUID, appID, and quiz status. IDPaas retains five pieces of PII data in the form of correct answers to the five questions of the quiz during the 60 minute window allowed for the user to finish the quiz. Outside of the window there is no PII. IDPaaS retains the USCIS ELIS token (the USCIS ELIS identifier) and ICAM UUID (the ICAM identifier) permanently. Identify user back to USCIS ELIS token so person can make changes to their account.

Length of retention of records is dependent on the requirements of the system ICAM is providing services for. As an example, in USCIS ELIS, a customer self-supplies information when establishing the account (name, home address, home phone number, mobile phone number, user name, user password, email address, alien number, and Department of State Case Id). Information is provided to USCIS ELIS not ICAM. ICAM creates a login account utilizing email as a username, and requiring email, phone number, or authentication application as a two-factor authentication method. ICAM is only email address or phone number. (UUID, email address, and phone number only information) As long as there is a USCIS ELIS account the account will be retained in ICAM.

Once their account is created, customers can then submit a benefit request. If no benefit request is submitted within 30 days of the account being created, the account is deleted and no account data persists. Information stays as long as there is an account in USCIS ELIS.

IDPaaS will verify the identity of a customer by asking multiple choice questions. The customer should know the answer to the questions and will prove identity by answer correctly. The customer will be presented with one correct and four incorrect answers to choose from. Upon answering, ICAM will send the responses back to IDPaaS for verification of the proofing process.

4(a) Does the project, program, or system retrieve information by personal identifier?	☐ No. Please continue to next question. ☒ Yes. If yes, please list all personal identifiers used: Personal identifiers are retrieved from the following sources to generate the IDPaaS quiz: • PCQS (A-number) • USCIS ELIS (ELIS token)

	The identifiers for USCIS ELIS is the token, which connects with the A-number and other profile information. The A-number is used to query PCQS.
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	☒ No. ☐ Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	N/A
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	N/A
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? *For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?*	☒ No. Please continue to next question. ☐ Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.	
N/A	

5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?	☐ No. ☒ Yes. If yes, please list: USCIS ELIS, PCQS
6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?	☒ No. IDPaaS receives DOS data from PCQS as well as USCIS ELIS. ☐ Yes. If yes, please list:
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	Existing Please describe applicable information sharing governance in place:

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.
[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.

	Department of State Memorandum of Understanding
7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?	☐ No. ☒ Yes. If yes, please list: USCIS Privileged User Training
8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals who have requested access to their PII?	☐ No. What steps will be taken to develop and maintain the accounting: ☒ **Yes.** In what format is the accounting maintained: USCIS customers have the opportunity to access their information online by logging into their account. The information they access includes a copy of the application they submitted, any notices or notifications generated by USCIS, and information about the status of their application.
9. Is there a FIPS 199 determination?[4]	☐ Unknown. ☐ No. ☒ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☒ Moderate ☐ High ☐ Undefined Integrity: ☐ Low ☒ Moderate ☐ High ☐ Undefined Availability: ☐ Low ☒ Moderate ☐ High ☐ Undefined

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	Jenny Hoots

[4] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

Date submitted to Component Privacy Office:	June 30, 2017
Date submitted to DHS Privacy Office:	July 14, 2017

Component Privacy Office Recommendation:
Please include recommendation below, including what new privacy compliance documentation is needed.

The USCIS Office of Privacy recommendation is to designate ICAM as a privacy sensitive system that requires PIA and SORN coverage because it contains PII from the public. The collection and maintenance of PII from the public precludes ICAM from a human resources only system designation.

Coverage for Customers Use (external):

- **DHS/USCIS/PIA-056 USCIS Electronic Immigration System (USCIS ELIS),** which covers the creation of online accounts by public users and the use IDPaaS for identity proofing purposes. USCIS is in the process of updating the USCIS ELIS PIA and plans to discuss the privacy risk associated with the back up code authenticator.

- **myE-Verify DHS/USCIS/PIA-030(e)** which covers the creation of online accounts by public users.

- **DHS/ALL-037 E-Authentication Records System of Records**, which covers members of the public, external stakeholders, and federal employees or contractors seeking electronic access to DHS programs and applications. This includes anyone attempting to authenticate his or her identity for the purpose of obtaining a credential to access a DHS program or application electronically, including when the program or application uses a third-party identity service provider to perform some or all credential management functions (e.g., prove identity, manage authentication tokens, and authenticate users).

Coverage for USCIS Employee/Contractor Use (internal):

- **DHS/ALL/PIA-014 - Personal Identity Verification (PIV) Management System,** which covers the issuance of credentials by DHS.

- **DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS)**, which covers employees and contractor access to DHS IT resources.

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	Kameron Cox
PCTS Workflow Number:	1148605
Date approved by DHS Privacy Office:	September 15, 2017
PTA Expiration Date	September 15, 2018

DESIGNATION

Privacy Sensitive System:	Yes If "no" PTA adjudication is complete.
Category of System:	IT System If "other" is selected, please describe: Click here to enter text.

Determination:

☐ PTA sufficient at this time.

☐ Privacy compliance documentation determination in progress.

☐ New information sharing arrangement is required.

☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies.

☒ Privacy Act Statement required.

☒ Privacy Impact Assessment (PIA) required.

☒ System of Records Notice (SORN) required.

☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer.

☐ A Records Schedule may be required. Contact your component Records Officer.

PIA:	**PIA update is required.** DHS/USCIS/PIA-030(e) E-Verify Program DHS/ALL/PIA-014(b) Personal Identity Verification (PIV) Management System Forthcoming update to DHS/USCIS/PIA-056 USCIS Electronic Immigration System
SORN:	**System covered by existing SORN** DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), November 27, 2012, 77 FR 70792 DHS/ALL-037 E-Authentication Records System of Records, August 11, 2014, 79 FR 46857

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above.

USCIS is submitting this PTA to document updates to its Identity, Credential, and Access Management (ICAM) system. ICAM provides USCIS employees and contractors with access to USCIS immigration systems and physical access to USCIS buildings through the employee's PIV card. ICAM also provides members of the public to USCIS online accounts through the use of two factor authentication processes.

The DHS Privacy Office (PRIV) concurs with USCIS Privacy that ICAM is a privacy sensitive system because it collects PII from members of the public, DHS employees and contractors, as well as employees of other government agencies. PRIV finds that PIA coverage is required for both internal and public facing systems of ICAM because its internal system collects PII from employees/contractors from more than one component, and its external system collects PII from members of the public.

PRIV agrees with USCIS that PIA coverage for the internal system of ICAM can be found in DHS/ALL/PIA-014(b) Personal Identity Verification (PIV) Management System, which covers the access to online USCIS systems through the use of DHS issued credentials.

PRIV finds that DHS/USCIS/PIA-030(e) E-Verify Program provides coverage for public customers and assess the privacy risks associated with using a third party service for a two factor authentication process to access online accounts. DHS/USCIS/PIA-056 USCIS Electronic Immigration System is utilized by MyUSCIS for its case management functionalities. PRIV agrees with USCIS Privacy that DHS/USCIS/PIA-056 requires an update to assess the use of the authenticator and backup code.

PRIV also finds that a SORN is required for use of the internal ICAM system because it accesses information by unique identifier. ICAM is covered by DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), because its purpose is to collect PII to allow DHS employees access to IT resources.

PRIV concludes that a SORN is also required for public use of ICAM because it accesses information by unique identifier. DHS/ALL-037 E-Authentication Records System of Records covers use and storage of limited PII in order to authenticate an individual's identity for the purpose of obtaining a credential to electronically access a DHS program or application. This system includes DHS programs or applications that use a third-party identity service provider to provide any of the credential services.

PRIV agrees with USCIS that A Privacy Notice must be provided at the point of information collection to notify the individual of the purpose, authority, and disclosures of the information collected. PRIV also agrees the notice should inform individuals to familiarize themselves with the privacy policy of the third party application they choose.

This PTA will expire in one year.

Appendix A

- Internal USCIS applications and systems currently supported by ICAM include:

Authentication (AuthN)

- Adobe Connect
- Application Name
- AWS Console
- Chef Delivery
- Cisco ISE
- CLAIMS4 WEB
- CloudBees Jenkins Enterprise
- Confidant Password Manager
- Deque/World Space
- DID(it) - AIOPS
- DID(it) App Store
- DID(it) ASC Drive Time
- DID(it) Asset Manager
- DID(it) AST Error Tracker
- DID(it) BADS
- DID(it) CAP Tracker
- DID(it) Discourse
- DID(it) EB-5 Database
- DID(it) ECHO
- DID(it) El Rescate (ERIA)
- DID(it) ELIS1 Archive
- DID(it) eSTAT
- DID(it) eWRTS
- DID(it) FAMS
- DID(it) FOD CSDB
- DID(it) FSNW
- DID(it) Grant Tracker
- DID(it) IMPACT
- DID(it) KEDL
- DID(it) LATS
- DID(it) Lynda
- DID(it) OIT HR Dashboard
- DID(it) Passport Tracker
- DID(it) PDCP
- DID(it) Pivotal Cloud Foundry
- DID(it) QADB
- DID(it) RAD
- DID(it) RAMT
- DID(it) Ride the Tide
- DID(it) Scheduler
- DID(it) Standard Dev Env
- DID(it) Union Time

- DSMS
- EDMS
- ELIS Admin
- ELIS Dashboard
- ELIS Jenkins
- ELIS SKY Applications
- ELIS2 Digital Evidence
- ELIS2 Internal App
- ESB PCQS
- ESB Vibe
- ESB VIBE Spring Boot
- FDNS-DS
- FileOnQ
- FIPS (Case360)
- FIPS Crystal Reports
- Fortify
- GitHub Enterprise
- GSS Chef
- ICAM myAccount Admin
- ICAM Pipeline Jenkins
- ICMS (Interim Case Management Solution)
- ICTS
- INFACT
- Innovation
- ITMS
- Jenkins Enterprise
- Jenkins Operations Center
- LeanKit
- Microservices Jenkins
- MSI Map
- myAccess
- myUSCIS Admin Panel
- MyUSCIS Command Center
- NASS Biometrics
- NASS InfoPass
- NASS Oauth
- NFTS
- NPS Web
- OMB Max
- Pivotal Cloud Foundry
- SalesForce
- ServiceNow
- SMART
- SPIDER/SPLUNK
- StatusPage.io
- TECS Audit
- Twistlock
- Vbrick

- VIS-SVS

Authorization (AuthZ)

- AWS Console
- CloudBees Jenkins Enterprise
- DID (it) App Store
- DID(it) BADS
- EDMS
- ELIS Dashboard
- ELIS Internal App
- ICAM Jenkins
- ICAM myAccount Admin
- myAccess
- myUSCIS Command Center
- NASS Adjudications
- NASS Biometrics
- SVS
- Twistlock