



PRIVACY THRESHOLD ANALYSIS (PTA)

This form serves as the official determination by the DHS Privacy Office to identify the privacy compliance requirements for all Departmental uses of personally identifiable information (PII).

A Privacy Threshold Analysis (PTA) serves as the document used to identify information technology (IT) systems, information collections/forms, technologies, rulemakings, programs, information sharing arrangements, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer, pursuant to Section 222 of the Homeland Security Act, and to assess whether there is a need for additional Privacy Compliance Documentation. A PTA includes a general description of the IT system, information collection, form, technology, rulemaking, program, pilot project, information sharing arrangement, or other Department activity and describes what PII is collected (and from whom) and how that information is used and managed.

Please complete the attached Privacy Threshold Analysis and submit 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

The Component Privacy Office will review this form and assess whether any privacy compliance documentation is required. If compliance documentation is required – such as Privacy Impact Assessment (PIA), System of Records Notice (SORN), Privacy Act Statement, or Computer Matching Agreement (CMA) – the Component Privacy Office will send you a copy of the relevant compliance template to complete and return.

This is a draft document that is pre-decisional, deliberative, and is designated For Official Use Only (FOUO). It is subject to the deliberative process privilege and attorney client privilege. It is not to be released, shared, or distributed outside of authorized channels without prior consultation and approval from the Department of Homeland Security (DHS) Privacy Office. Unauthorized disclosure may result in administrative, civil, or criminal penalties.

This is a draft document that is pre-decisional, deliberative, and is designated For Official Use Only (FOUO). It is subject to the deliberative process privilege and attorney client privilege. It is not to be released, shared, or distributed outside of authorized channels without prior consultation and approval from the Department of Homeland Security (DHS) Privacy Office. Unauthorized disclosure may result in administrative, civil, or criminal penalties.



Privacy Threshold Analysis (PTA)

Specialized Template for Information Collections (IC) and Forms

The Forms-PTA is a specialized template for Information Collections and Forms. This specialized PTA must accompany all Information Collections submitted as part of the Paperwork Reduction Act process (any instrument for collection (form, survey, questionnaire, etc.) from ten or more members of the public). Components may use this PTA to assess internal, component-specific forms as well.

Form Number:	Click here to enter text.		
Form Title:	Communication Assets Survey & Mapping (CASM) Tool User Registration and Communications Unit (COMU) Training		
Component:	Cybersecurity and Infrastructure Security Agency (CISA)	Office:	Emergency Communications Division (ECD)

IF COVERED BY THE PAPERWORK REDUCTION ACT:

Collection Title:	Communication Assets Survey & Mapping (CASM) Tool		
OMB Control Number:	1670-0043	OMB Expiration Date:	October 31, 2026
Collection status:	Extension	Date of last PTA (if applicable):	June 4, 2024

PROJECT OR PROGRAM MANAGER

Name:	Scott Eder
--------------	------------

This is a draft document that is pre-decisional, deliberative, and is designated For Official Use Only (FOUO). It is subject to the deliberative process privilege and attorney client privilege. It is not to be released, shared, or distributed outside of authorized channels without prior consultation and approval from the Department of Homeland Security (DHS) Privacy Office. Unauthorized disclosure may result in administrative, civil, or criminal penalties.



Office:	Office of the Chief Information Officer	Title:	Section Chief Cyber Mission Data and Applications
Phone:	202 669-4672	Email:	scott.eder@cisa.dhs.gov
Name:	Anais Azoulay		
Office:	Emergency Communications Division	Title:	IT Cyber Security Specialist
Phone:	202 704-5289	Email:	anais.azoulay@cisa.dhs.gov

COMPONENT INFORMATION COLLECTION/FORMS CONTACT

Name:	Benjamin Thomsen		
Office:	Office of the Chief Information officer	Title:	IT Cybersecurity Program Manager
Phone:	202 880-5434	Email:	benjamin.thomsen@cisa.dhs.gov

This is a draft document that is pre-decisional, deliberative, and is designated For Official Use Only (FOUO). It is subject to the deliberative process privilege and attorney client privilege. It is not to be released, shared, or distributed outside of authorized channels without prior consultation and approval from the Department of Homeland Security (DHS) Privacy Office. Unauthorized disclosure may result in administrative, civil, or criminal penalties.



SPECIFIC IC/Forms PTA QUESTIONS

1. Purpose of the Information Collection or Form

- a. Describe the purpose of the information collection or form. *Please provide a general description of the project and its purpose, including how it supports the DHS mission, in a way a non-technical person could understand (you may use information from the Supporting Statement).*

If this is an updated PTA, please specifically describe what changes or upgrades are triggering the update to this PTA.

The CISA Office of Privacy, Access, Civil Liberties and Transparency (PACT) is submitting this PTA as these forms go through a Paperwork Reduction Act (PRA) renewal. Changes made since the previous PTA include the new individuals listed as Program Managers and Information Collection/Forms contacts, the expiration of the Inter-Agency Agreement (IAA) that supported the tool, and amended authority citations in the PTA and Privacy Act Statements to better align with program-specific activities.

Per National Emergency Communications Plan (NECP) requirements, CISA's Emergency Communications Division (ECD) provides the CASM tool, accessible by StateWide Interoperability Coordinators (SWICs), via <https://login.casm.cisa.dhs.gov>. The National Emergency Communications Plan Initiative 1.3 "makes available an effective communications asset management tool containing security and privacy controls to allow for nationwide intergovernmental use." CASM supports tactical planning among Federal, State, local, and tribal governments at the regional interstate level. Access to State/territory CASM accounts are controlled by the respective SWIC for their State/territory.

CASM Access Request Form

In order to receive an account to access CASM, SWICs must request access via the CASM Access Request Form (see screenshot below). Information is collected, entered into, and maintained in the tool, which is operated by the CISA Office of the Chief Information

This is a draft document that is pre-decisional, deliberative, and is designated For Official Use Only (FOUO). It is subject to the deliberative process privilege and attorney client privilege. It is not to be released, shared, or distributed outside of authorized channels without prior consultation and approval from the Department of Homeland Security (DHS) Privacy Office. Unauthorized disclosure may result in administrative, civil, or criminal penalties.



Officer (OCIO) on behalf of ECD. This task was previously performed by the U.S. Navy Information Warfare Center (NIWC) Pacific under an IAA that the agency opted not to extend. The image included at the end of this PTA shows the current CASM access request form. The form collects a prospective user's first and last name, email address, home organization, and the organization and type of data that the prospective user is requesting access to. It also asks them to provide their manager's (supervisor) email address or phone number.

Communications Unit (COMU) Training Information Collection

ECD, in accordance with the NECP, fosters the development of interoperable emergency communications capabilities for State, regional, local, and tribal organizations. One way ECD achieves this goal is by offering All Hazards Communications Unit training courses for State, regional, and local emergency response stakeholders. Participation in these courses requires satisfaction of several prerequisites that the States/territories verify for their nominated students. COMU students provide basic contact information (name, organization affiliation, mailing address, email address, and phone number) to the SWIC, which is then entered into CASM. The contact information that is provided is only used to document attendance and so the student can receive a certificate of completion for the training course. ECD does not retrieve COMU student information by personal identifier. COMU records can only be retrieved by state, course title, and/or date.

- b. List the DHS (or Component) authorities to collect, store, and use this information. *If this information will be stored and used by a specific DHS component, list the component-specific authorities.*

6 U.S.C. 652(c)(11) and 571(c)(5)

2. Describe the IC/Form

This is a draft document that is pre-decisional, deliberative, and is designated For Official Use Only (FOUO). It is subject to the deliberative process privilege and attorney client privilege. It is not to be released, shared, or distributed outside of authorized channels without prior consultation and approval from the Department of Homeland Security (DHS) Privacy Office. Unauthorized disclosure may result in administrative, civil, or criminal penalties.



a. Does this form collect any Personally Identifiable Information” (PII ¹)?	☒ Yes ☐ No
b. From which type(s) of individuals does this form collect information? (<i>Check all that apply.</i>)	☒ Members of the public ☒ U.S. citizens or lawful permanent residents ☐ Non-U.S. Persons ☒ DHS Employees/Contractors (list Components) <ul style="list-style-type: none">• CISA• FEMA• USCG ☒ Other federal employees or contractors
c. Who will complete and submit this form? (<i>Check all that apply.</i>)	☒ The record subject of the form (e.g., the individual applicant). ☐ Legal Representative (preparer, attorney, etc.). ☐ Business entity. If a business entity, is the only information collected business contact information? ☐ Yes ☐ No ☐ Law enforcement. ☒ DHS employee/contractor. ☐ Other individual/entity/organization that is NOT the record subject. <i>Please describe.</i> Click here to enter text.

¹ Personally identifiable information means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which 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.

This is a draft document that is pre-decisional, deliberative, and is designated For Official Use Only (FOUO). It is subject to the deliberative process privilege and attorney client privilege. It is not to be released, shared, or distributed outside of authorized channels without prior consultation and approval from the Department of Homeland Security (DHS) Privacy Office. Unauthorized disclosure may result in administrative, civil, or criminal penalties.



d. How do individuals complete the form? <i>Check all that apply.</i>	☒ Paper. ☐ Electronic. (ex: fillable PDF) ☒ Online web form. (available and submitted via the internet) <i>Provide link:</i> https://login.casm.cisa.dhs.gov
e. What information will DHS collect on the form? <i>List all individual PII data elements on the form. If the form will collect information from more than one type of individual, please break down list of data elements collected by type of individual.</i>	
Prospective CASM Users: First and last name, email address, organization affiliation, organization to be accessed, and type of data to be accessed. Prospective CASM User's Manager (Supervisor): Email address and phone number. COMU Training Participants: Name, organization affiliation, mailing address, email address, and phone number	
f. Does this form collect Social Security number (SSN) or other element that is stand-alone Sensitive Personally Identifiable Information (SPII)? <i>Check all that apply.</i>	
☐ Social Security number ☐ Alien Number (A-Number) ☐ Tax Identification Number ☐ Visa Number ☐ Passport Number ☐ Bank Account, Credit Card, or other financial account number ☐ Other. <i>Please list:</i>	☐ DHS Electronic Data Interchange Personal Identifier (EDIPI) ☐ Social Media Handle/ID ☐ Known Traveler Number ☐ Trusted Traveler Number (Global Entry, Pre-Check, etc.) ☐ Driver's License Number ☐ Biometrics

This is a draft document that is pre-decisional, deliberative, and is designated For Official Use Only (FOUO). It is subject to the deliberative process privilege and attorney client privilege. It is not to be released, shared, or distributed outside of authorized channels without prior consultation and approval from the Department of Homeland Security (DHS) Privacy Office. Unauthorized disclosure may result in administrative, civil, or criminal penalties.



g. List the <i>specific authority</i> to collect SSN or these other SPII elements.	
N/A	
h. How will the SSN and SPII information be used? What is the purpose of the collection?	
N/A	
i. Is SSN necessary to carry out the functions of this form and/or fulfill requirements of the information collection? <i>Note:</i> even if you are properly authorized to collect SSNs, you are required to use an alternative identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, privacy-enhancing alternatives should be taken, such as truncating the SSN.	
N/A	
j. Are individuals provided notice at the time of collection by DHS (<i>Does the records subject have notice of the collection or is form filled out by third party</i>)?	☒ Yes. Please describe how notice is provided. A Privacy Act Statement is provided on the landing page where the CASM access request form can be found. A statement is also provided on the CASM/COMU Training Information Collection. ☐ No.

3. How will DHS store the IC/form responses?	
a. How will DHS store the original, completed IC/forms?	☒ Paper. Please describe. COMU Training forms are generally filled out on paper at training sites and are later added into the CASM system through manual data entry.

This is a draft document that is pre-decisional, deliberative, and is designated For Official Use Only (FOUO). It is subject to the deliberative process privilege and attorney client privilege. It is not to be released, shared, or distributed outside of authorized channels without prior consultation and approval from the Department of Homeland Security (DHS) Privacy Office. Unauthorized disclosure may result in administrative, civil, or criminal penalties.



	<p>☒ Electronic. Please describe the IT system that will store the data from the form. Access request forms are electronically submitted directly into the CASM tool.</p> <p>☐ Scanned forms (completed forms are scanned into an electronic repository). Please describe the electronic repository. Click here to enter text.</p>
b. If electronic, how does DHS input the responses into the IT system?	<p>☒ Manually (data elements manually entered). Please describe. Data from completed paper forms is added manually by ECD.</p> <p>☒ Automatically. Please describe. When a user submits an electronic access request form, it is automatically submitted directly into the CASM tool.</p>
c. How would a user search the information submitted on the forms, i.e., how is the information retrieved?	<p>☒ By a unique identifier.² Please describe. If information is retrieved by personal identifier, please submit a Privacy Act Statement with this PTA. CASM users can be searched by personal or non-personal identifiers within the system (name, title, organization, email address).</p> <p>☐ By a non-personal identifier. Please describe. Click here to enter text.</p>

² Generally, a unique identifier is considered any type of "personally identifiable information," meaning any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which 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.

This is a draft document that is pre-decisional, deliberative, and is designated For Official Use Only (FOUO). It is subject to the deliberative process privilege and attorney client privilege. It is not to be released, shared, or distributed outside of authorized channels without prior consultation and approval from the Department of Homeland Security (DHS) Privacy Office. Unauthorized disclosure may result in administrative, civil, or criminal penalties.



d. What is the records retention schedule(s)? <i>Include the records schedule number.</i>	General Records Schedule (GRS) 3.2: System Access Records . These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. Includes records such as: user profiles, log-in files, password files, audit trail files and extracts, system usage files, cost-back files used to assess charges for system use.
e. How do you ensure that records are disposed of or deleted in accordance with the retention schedule?	User access records are deleted from the system when business use ceases.
f. Is any of this information shared outside of the original program/office? <i>If yes, describe where (other offices or DHS components or external entities) and why. What are the authorities of the receiving party?</i>	
☐ Yes, information is shared with other DHS components or offices. Please describe. Click here to enter text.	
☐ Yes, information is shared <i>external</i> to DHS with other federal agencies, state/local partners, international partners, or non-governmental entities. Please describe. Click here to enter text.	
☒ No. Information on this form is not shared outside of the collecting office. User information is available to other CASM users (who could work for other DHS components, federal agencies, state/local partners, etc.); however, the information will not otherwise be shared outside of the CASM tool.	

This is a draft document that is pre-decisional, deliberative, and is designated For Official Use Only (FOUO). It is subject to the deliberative process privilege and attorney client privilege. It is not to be released, shared, or distributed outside of authorized channels without prior consultation and approval from the Department of Homeland Security (DHS) Privacy Office. Unauthorized disclosure may result in administrative, civil, or criminal penalties.



Please include a copy of the referenced form and Privacy Act Statement/Privacy Notice (if applicable) with this PTA upon submission.

PTA REVIEW
(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE REVIEWER)

Component Privacy Office Reviewer:	Jacob Curry
Date submitted to Component Privacy Office:	April 28, 2026
Concurrence from other Components involved (if applicable):	Click here to enter text.
Do you have an approved a Privacy Act Statement/Privacy Notice for this form?	☒ Yes. Please include it with this PTA submission. ☐ No. Please describe why not. Click here to enter text.
Component Privacy Office Recommendation: <i>Please include recommendation below, including what existing privacy compliance documentation is available or new privacy compliance documentation is needed.</i>	
CISA is completing this PTA to discuss updates to the CASM Registration and COMU Training information collections managed by ECD. These collections are used to provide stakeholders access to the CASM tool and facilitate participation in agency-offered emergency communications trainings. PII is collected to fulfill both purposes. Changes to note since the previous PTA include new program contacts, the expiration of the Inter-	

This is a draft document that is pre-decisional, deliberative, and is designated For Official Use Only (FOUO). It is subject to the deliberative process privilege and attorney client privilege. It is not to be released, shared, or distributed outside of authorized channels without prior consultation and approval from the Department of Homeland Security (DHS) Privacy Office. Unauthorized disclosure may result in administrative, civil, or criminal penalties.



Agency Agreement (IAA) that supported the CASM tool, and amended authority citations in the PTA and Privacy Act Statements

The PACT reviewer recommends that these continue to be considered privacy-sensitive collections, requiring both PIA and SORN coverage.

Recommended PIA coverage remains DHS/ALL/PIA-006 DHS General Contacts List, which deals with the collection of contact information to conduct agency operations.

SORN coverage is required because information is retrieved by unique identifiers. Recommended SORN coverage remains:

DHS/ALL – 002 Department of Homeland Security (DHS) Mailing and Other Lists System, November 25, 2008, 73 FR 71659; this SORN provides for records of contact information given by persons who attend or have interest in DHS programs, training courses, and events.

DHS/ALL – 004 General Information Technology Access Account Records System (GITAARS), November 27, 2012, 77 FR 70792, which covers the collection of information to provide authorized individuals access to DHS information technology resources, such as CASM.

PTA ADJUDICATION

(TO BE COMPLETED BY THE DHS COMPONENT PRIVACY OFFICE APPROVER)

Component Privacy Office Approver:	James Burd
PTA Approved Date:	June 8, 2026
PTA Expiration Date:	June 7, 2029

DESIGNATION

**JAMES C
BURD**

Digitally signed by JAMES C
BURD
Date: 2026.06.08 17:28:45
-04'00'

This is a draft document that is pre-decisional, deliberative, and is designated For Official Use Only (FOUO). It is subject to the deliberative process privilege and attorney client privilege. It is not to be released, shared, or distributed outside of authorized channels without prior consultation and approval from the Department of Homeland Security (DHS) Privacy Office. Unauthorized disclosure may result in administrative, civil, or criminal penalties.



Privacy Sensitive IC or Form:	Yes If “no” PTA adjudication is complete.
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 SPII applies. ☒ Privacy Act Statement required. ☒ Privacy Impact Assessment (PIA) required. ☒ System of Records Notice (SORN) required. ☐ Specialized training required. ☐ Other. Click here to enter text.
Privacy Act Statement:	e(3) statement update is required. The attached updated e(3) statement is approved.
System PTA:	No system PTA required. Click here to enter text.
PIA:	System covered by existing PIA If covered by existing PIA, please list: DHS/ALL/PIA-006 DHS General Contacts List If a PIA update is required, please list: Click here to enter text.
SORN:	System covered by existing SORN If covered by existing SORN, please list: DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, November 25, 2008, 73 FR 71659; DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), November 27, 2012, 77 FR 70792 If a SORN update is required, please list: Click here to enter text.
Component Privacy Office Adjudication: <i>Please describe rationale for privacy compliance determination above.</i>	

This is a draft document that is pre-decisional, deliberative, and is designated For Official Use Only (FOUO). It is subject to the deliberative process privilege and attorney client privilege. It is not to be released, shared, or distributed outside of authorized channels without prior consultation and approval from the Department of Homeland Security (DHS) Privacy Office. Unauthorized disclosure may result in administrative, civil, or criminal penalties.



CISA is submitting this PTA renewal for the CASM user registration and COMU training information collection, and to document the minor administrative changes that have occurred since the last PTA. The purpose of the CASM tool is to provide a national interoperable emergency communications inventory for public safety agencies in all states and territories with the capability to contribute, visualize, and share communications asset information. CASM identifies land mobile radio (LMR) and other technology resources currently in use, as well as Communication Unit (COMU) information that allows users to document attendance of emergency communications training courses, for public safety communications operability and interoperability planning. Changes made since the previous PTA include the new individuals listed as Program Managers and Information Collection/Forms contacts, the expiration of the Inter-Agency Agreement (IAA) that supported the tool, and amended authority citations in the PTA and Privacy Act Statements to better align with program-specific activities.

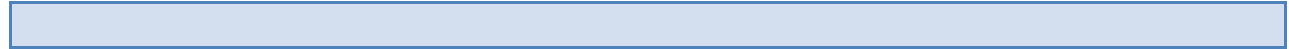
The CISA privacy officer has determined this continues to be privacy sensitive, requiring PIA and SORN coverage.

PIA coverage is provided by DHS/ALL/PIA-006 DHS General Contact Lists, which covers the collection of contact information to conduct agency operations.

SORN coverage is required because information is retrieved by a unique identifier. SORN coverage is provided by DHS/ALL-002 - Department of Homeland Security (DHS) Mailing and Other Lists System, which covers the lists used to facilitate mailings to multiple addressees and other activities in furtherance of DHS duties. Additionally, DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), which allows for the collection of information to provide authorized individuals access to, or interact with DHS information technology resources, and allow DHS to track use of DHS IT resources.

The attached updated e(3) statement is approved.

This is a draft document that is pre-decisional, deliberative, and is designated For Official Use Only (FOUO). It is subject to the deliberative process privilege and attorney client privilege. It is not to be released, shared, or distributed outside of authorized channels without prior consultation and approval from the Department of Homeland Security (DHS) Privacy Office. Unauthorized disclosure may result in administrative, civil, or criminal penalties.



This is a draft document that is pre-decisional, deliberative, and is designated For Official Use Only (FOUO). It is subject to the deliberative process privilege and attorney client privilege. It is not to be released, shared, or distributed outside of authorized channels without prior consultation and approval from the Department of Homeland Security (DHS) Privacy Office. Unauthorized disclosure may result in administrative, civil, or criminal penalties.



To be used for CISA ECD to request to register individuals for training purposes:

Privacy Act Statement:

Authority: 6 U.S.C. § 652 (c)(11) and §571(c)(5) authorize the collection of this information.

Purpose: The purpose for this collection is to allow the Cybersecurity and Infrastructure Security Agency (CISA) to register you for training.

Routine Uses: The information collected may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes using the information as necessary and authorized by the routine uses published in DHS/ALL-002 – Department of Homeland Security (DHS) Mailing and Other Lists System (November 25, 2008, 73 FR 71659).

Disclosure: Providing this information is voluntary, however, failure to provide this information may prevent or delay CISA from processing your registration request.

To be used to grant CISA ECD Statewide Interoperability Coordinators access to a DHS system, the Communication Assets Survey and Mapping (CASM) Tool

Privacy Act Statement:

Authority: 6 U.S.C. § 652 (c)(11) and §571(c)(5) authorize the collection of this information.

Purpose: The primary purpose of this collection is to provide you with access to a Cybersecurity and Infrastructure Security Agency (CISA) system.

Routine Uses: The information collected may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes using the information as necessary and authorized by the routine uses published in DHS/ALL-004 General Information Technology Access Account Records System of Records (September 29, 2009, 74 FR 49882).

Disclosure: Providing this information is voluntary, however, failure to provide this information may prevent or delay CISA from processing your request for access.

This is a draft document that is pre-decisional, deliberative, and is designated For Official Use Only (FOUO). It is subject to the deliberative process privilege and attorney client privilege. It is not to be released, shared, or distributed outside of authorized channels without prior consultation and approval from the Department of Homeland Security (DHS) Privacy Office. Unauthorized disclosure may result in administrative, civil, or criminal penalties.



Request New Access

First Name

First Name required

Last Name *

Last Name required

Email *

Email required

Home Organization *

Home Organization required

Manager Name *

Manager Name required

Manager Email or Phone *

Manager Email/Phone
required

Type of Data to Access *

☐ Agency Data

☐ COMM Asset Data

Organization to Access *

Select Organization

Reason for Request *

Reason required

☐

I'm not a robot



reCAPTCHA
Privacy * Terms

Cancel

* Required Fields

Submit Request

This is a draft document that is pre-decisional, deliberative, and is designated For Official Use Only (FOUO). It is subject to the deliberative process privilege and attorney client privilege. It is not to be released, shared, or distributed outside of authorized channels without prior consultation and approval from the Department of Homeland Security (DHS) Privacy Office. Unauthorized disclosure may result in administrative, civil, or criminal penalties.