



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. After review by your component Privacy Officer the PTA is sent to the Department's Senior Director for Privacy Compliance for action. 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 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 DHS Privacy Office or component Privacy Office will send you a copy of the relevant compliance template to complete and return.



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: 1670-0046

Form Title: SAFECOM Membership Questionnaire

Component:	Cybersecurity and Infrastructure Security Agency (CISA)	Office:	Emergency Communications Division (ECD)
------------	---	---------	--

IF COVERED BY THE PAPERWORK REDUCTION ACT:

Collection Title: SAFECOM Membership Questionnaire

OMB Control Number:	1670-0046	OMB Expiration Date:	July 31, 2025
Collection status:	New Collection	Date of last PTA (if applicable):	July 7, 2020

PROJECT OR PROGRAM MANAGER

Name:	Georgia Anagnostopoulos		
Office:	ECD	Title:	PRA Manager
Phone:	240-409-4798	Email:	georgia.anagnostopoulos@associates.cisa.dhs.gov

COMPONENT INFORMATION COLLECTION/FORMS CONTACT

Name: Benjamin Thomsen



Office:	Office of the Chief Information Officer (OCIO)	Title:	IT Cybersecurity Program Manager
Phone:	202-254-7179	Email:	CISA.PRA@hq.dhs.gov

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.*

PACT is submitting this PTA in line with the three-year expiration cycle and to document updates to the SAFECOM Membership Questionnaire that have occurred since its initial PTA in July 2020. The only changes to note at this time are to the project manager and information collection contacts.

Through collaboration with emergency responders and elected officials across all levels of government, the Assuring a Safer America Through Effective Public Safety Communications (SAFECOM) program works to improve emergency response providers' inter- jurisdictional and interdisciplinary emergency communications interoperability across local, regional, tribal, state, territorial, international borders, and with federal government entities. SAFECOM works with existing federal communications programs and key emergency response stakeholders to address the need to develop better technologies and processes for the coordination of existing communications systems and future networks.

Through these partnerships, SAFECOM has created key documents such as the Interoperability Continuum, the Statement of Requirements (SoR) for baseline communications and interoperability standards, the Statewide Communication Interoperability Plan (SCIP) Methodology, and the National Emergency Communications Plan (NECP) to assist emergency responders nationwide with improving communications and interoperability.

The purpose of the SAFECOM Membership Questionnaire is a nationwide data collection effort to obtain actionable and critical data that drives our nation's emergency communication policies, programs, and funding. SAFECOM will



leverage the collected data to identify individuals with specific expertise and inform development of the program's strategic priorities.

The questionnaire, submitted bi-annually or upon new membership to SAFECOM, is designed to identify membership gaps, obtain updated information on SAFECOM's membership body (e.g., public safety communications experience, accomplishments, acquired skills/certifications, etc.), update SAFECOM resources in order to be in line with the current state of the nation's emergency communications.

SAFECOM seeks responses from emergency response provider organizations at the federal, state, local, and territory levels of government, as well as Tribal Nations with:

- **A public safety-related mission in the following four disciplines: Law Enforcement, Fire & Rescue, Emergency Medical Services (EMS), and Public Safety Answering Points (PSAPs)/Public Safety Communications Centers (PSCCs).**
- **Users of public safety communications technology during day-to-day and out-of- the-ordinary situations.**

The personal contact information collected in section one of the questionnaire will be inputted into the SAFECOM Internal Membership Profile Tracker, a database directory housed on SAFECOM's dedicated space on HSIN accessible to all SAFECOM members in order to facilitate communication and collaboration between members.

- 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.*

Public Law 109-296, Title VI, §671(b), Title XVIII, §1801(c)(2)

2. Describe the IC/Form



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? (Check all that apply.)	☒ Members of the public ☒ U.S. citizens or lawful permanent residents ☐ Non-U.S. Persons ☒ DHS Employees/Contractors CISA ☒ Other federal employees or contractors
c. Who will complete and submit this form? (Check all that apply.)	☒ 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. Please describe. Click here to enter text.
d. How do individuals complete the form? Check all that apply.	☒ Paper. ☒ Electronic. (ex: fillable PDF) ☐ Online web form. (available and submitted via the internet) Provide link:

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.



e. What information will DHS collect on the form? *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.*

, Full name, email, phone number, city and state of residence, biography (user will upload a copy of their bio/resume listing their experience and accomplishments. Upload can be in PDF or docx format), LinkedIn contact information, tenure (active/retired). Social Media platforms used?

The questionnaire itself is strictly voluntary. Responses nor membership into SAFECOM is required. Respondents may submit responses to any of the data elements for the use of SAFECOM to use in its database of public safety experience. Individuals may also voluntarily provide memberships, national associations, organizations, special interest groups, education, volunteer experience, etc. Such voluntary responses will allow SAFECOM to update its database in with accurate contact information and capabilities of emergency response providers.

f. Does this form collect Social Security number (SSN) or other element that is stand-alone Sensitive Personally Identifiable Information (SPII)? *Check all that apply.*

- | | |
|--|--|
| ☐ Social Security number | ☐ DHS Electronic Data Interchange |
| ☐ Alien Number (A-Number) | Personal Identifier (EDIPI) |
| ☐ Tax Identification Number | ☐ Social Media Handle/ID |
| ☐ Visa Number | ☐ Known Traveler Number |
| ☐ Passport Number | ☐ Trusted Traveler Number (Global |
| ☐ Bank Account, Credit Card, or other | Entry, Pre-Check, etc.) |
| financial account number | ☐ Driver's License Number |
| ☐ Other. <i>Please list:</i> | ☐ Biometrics |

g. List the ***specific authority*** 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: 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.</i> Click here to enter text.	
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. Notice is provided to individuals as per the Privacy Act Statement on the SAFECOM Questionnaire form itself and with the PRA Burden Statement. ☐ No.

3. How will DHS store the IC/form responses?	
a. How will DHS store the original, completed IC/forms?	☒ Paper. Please describe. <i>All paper submissions will be stored in a locked file cabinet. Paper submissions will be used with members cannot or do not have adequate access to the electronic questionnaire. Paper submissions will be transcribed by CISA/ECD into the SAFECOM databased located in HSIN, and once inputted the paper submission will be shredded securely by CISA/ECD.</i> ☒ Electronic. Please describe the IT system that will store the data from the form. <i>All electronic submissions will be stored on SAFECOM's dedicated space on the Homeland Security Information Network (HSIN) accessed only by SAFECOM members.</i>



	☐ Scanned forms (completed forms are scanned into an electronic repository). Please describe the electronic repository. Click here to enter text.
b. If electronic, how does DHS input the responses into the IT system?	☐ Manually (data elements manually entered). Please describe. Click here to enter text. ☒ Automatically. Please describe. <i>The Questionnaire is a fillable PDF. All submissions will be uploaded and stored on the Homeland Security Information Network (HSIN).</i>
c. How would a user search the information submitted on the forms, i.e., how is the information retrieved?	☒ By a unique identifier. ² Please describe. If information is retrieved by personal identifier, please submit a Privacy Act Statement with this PTA. <i>Search by first and/or last name</i> ☒ By a non-personal identifier. Please describe. <i>City and State of location</i>
d. What is the records retention schedule(s)? <i>Include the records schedule number.</i>	The information collected by SAFECOM will be retained in accordance with NARA General Records Schedule (GRS) GRS 5.3, Item 020 (DAA-GRS-2016-0004-0002) - Employee emergency contact information.
e. How do you ensure that records are disposed of or deleted in accordance with the retention schedule?	In accordance with the records schedule DAA-GRS-2016-0004-0002, records are to be destroyed when superseded or obsolete, or upon separation of the individual from SAFECOM membership.
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>	

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.



☒ Yes, information is shared with other DHS components or offices. Please describe.

Information derived from the SAFECOM Questionnaire, is available in the SAFECOM Internal Membership Profile Tracker, to all approved CISA users of HSIN or by request via email at SAFECOMGovernance@cisa.dhs.gov.

☒ Yes, information is shared *external* to DHS with other federal agencies, state/local partners, international partners, or non-governmental entities. Please describe.

The information on the SAFECOM Internal Membership Profile Tracker, is also available to non-DHS SAFECOM Members with HSIN access or by request via email at SAFECOMGovernance@cisa.dhs.gov.

☐ No. Information on this form is not shared outside of the collecting office.



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



PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	Jacob Curry
Date submitted to Component Privacy Office:	December 7, 2023
Concurrence from other Components involved (if applicable):	Click here to enter text.
Date submitted to DHS Privacy Office:	December 8, 2023
Have you approved a Privacy Act Statement for this form? (<i>Only applicable if you have received a waiver from the DHS Chief Privacy Officer to approve component Privacy Act Statements.</i>)	☒ 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>	
The CISA Office of Privacy, Access, Civil Liberties and Transparency (PACT) is submitting this PTA for the SAFECOM Membership Questionnaire, in order to document the non-substantive changes that have occurred since the initial 2020 PTA and renew the compliance cycle. The questionnaire is a nationwide data collection effort to obtain actionable and critical data that drives our nation's emergency communication policies, programs, and funding. SAFECOM will leverage the collected data to update the membership body as well as identify gaps and inform development of the program's strategic priorities. PACT recommends that the SAFECOM Membership Questionnaire is privacy sensitive, requiring PIA coverage due to the collection of PII. SORN coverage is also required because the data collected can be retrieved through the use of a unique identifier.	



PACT recommends that PIA coverage be provided by DHS/ALL/PIA-006 DHS General Contacts List.

PACT recommends that SORN coverage be provided by DHS/ALL-002 Department of Homeland Security (DHS) Mailing and other Lists.

PRIVACY THRESHOLD ADJUDICATION

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	Brian Pochatila
PCTS Workflow Number:	0016024
Date approved by DHS Privacy Office:	January 24, 2024
PTA Expiration Date	January 24, 2027
DHS Privacy Office Approver (if applicable):	Riley Dean

DESIGNATION

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 currently accurate. PAS submitted and approved.
System PTA:	Choose an item. 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; DHS/ALL/PIA-061 HSIN 3.0 Shared Spaces On The Sensitive But Unclassified Network; DHS/ALL/PIA-069 DHS Surveys, Interviews, and Focus Groups 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 If a SORN update is required, please list: Click here to enter text.
DHS Privacy Office Comments: <i>Please describe rationale for privacy compliance determination above.</i>	
CISA is submitting this PTA renewal for the SAFECOM Membership Questionnaire, which is a nationwide data collection effort to obtain actionable and critical data that drives the nation's emergency communication policies, programs, and funding. SAFECOM will leverage the collected data to update the membership body as well as identify gaps and inform development of the program's strategic priorities. The only changes to note at this time are to the project manager and information collection contacts and the questionnaire has been updated to remove for individuals to submit headshot photos. The questionnaire collects personally identifiable information of personal contact information that will be inputted into the SAFECOM's Internal Membership Profile Tracker and SAFECOM's directory on HSIN. The survey information is only deleted when business use ceases, so if a person is no longer a member of SAFECOM then their information will be deleted. The DHS Privacy Office finds that this questionnaire is privacy sensitive requiring PIA and SORN coverage. PIA coverage is provided by: DHS/ALL/PIA-006 DHS General Contacts List collects a minimal amount of contact information in order to distribute information and perform various other administrative tasks.	



- DHS/ALL/PIA-061 HSIN 3.0 Shared Spaces On The Sensitive But Unclassified Network enables information sharing on HSIN.
- DHS/ALL/PIA-069 DHS Surveys, Interviews, and Focus Groups permits DHS and its Components to periodically solicit voluntary feedback from its employees, contractors, external stakeholders, and the general public through the use of surveys, interviews, and focus groups to improve DHS services and operations.

SORN coverage is provided By DHS/ALL-002 DHS Mailing and Other Lists System, which maintains lists of individuals who are members.