



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:	1670-0027		
Form Title:	1670-New Emergency Response Operations Stakeholder Feedback Form		
Component:	Cybersecurity and Infrastructure Security Agency (CISA)	Office:	Integrated Operations Division (IOD) Emergency Response Operations (ERO) Branch

IF COVERED BY THE PAPERWORK REDUCTION ACT:

Collection Title:	Emergency Response Operations Stakeholder Feedback Form		
OMB Control Number:	1670-0027	OMB Expiration Date:	Click here to enter a date.
Collection status:	New Collection	Date of last PTA (if applicable):	Click here to enter a date.

PROJECT OR PROGRAM MANAGER

Name:	John O'Connor		
Office:	Emergency Response Operations	Title:	Branch Chief
Phone:	(703) 235-5028	Email:	john.oconnor@cisa.dhs.gov



COMPONENT INFORMATION COLLECTION/FORMS CONTACT

Name:	John Campbell		
Office:	OCIO	Title:	Planning Administration (PLAD), Section 508/PRA
Phone:	(202) 689-5621	Email:	John.Campbell@cisa.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.

CISA Central is CISA’s hub for staying on top of threats and emerging risks to our nation’s critical infrastructure, whether they are of cyber, communications or physical origin. CISA Central is the simplest, most centralized way for critical infrastructure partners and stakeholders to engage with CISA and is the easiest way for all critical infrastructure stakeholders to request assistance and get the information they need to understand the constantly evolving risk landscape.

Through CISA Central, CISA coordinates situational awareness and response to national cyber, communications, and physical incidents. CISA works closely with public, private sector, and international partners, offering technical assistance, information security and education to protect our nation’s critical infrastructure from a broad range of current cyber, communication, and physical threats.

Within CISA Central, the Emergency Response Operations (ERO) Branch performs emergency support functions to support CISA's roles as the Emergency Support Function (ESF) Coordinator and Co-Primary Agency (along with FEMA) to support regional and national disasters, supports Continuity and National Security Emergency Preparedness, and serves as the Communications Information Sharing and Analysis Center (ISAC) for the following:

- *Emergency Support Function (ESF) #2 – Communications*
- *ESF #14 – Cross Sector Business and Infrastructure*

Continuity and National Security Emergency Preparedness



- *Plans, analyzes, conducts testing, and maintains responsibility for several operational capabilities for the Federal Executive Branch.*

National Coordinating Center for Telecommunications - Communications ISAC

- *Organization by which the Federal Government and communications industry jointly prepare for and maintain readiness to respond to emergency communications service requirements.*

CISA Central's ERO interacts with a variety of stakeholders across multiple mission areas. The purpose of the surveys is to capture stakeholder feedback on shared products to ensure value to recipients and to guide and improve future products and processes. Collectively potential survey respondents include Federal Departments and Agencies that support or need disaster response situational awareness; State, Local, Territorial, and Tribal (SLTT) entities supported by Federal response efforts; Federal partner entities with continuity communications missions; International partners addressing infrastructure protection; communications industry partners supporting resilient communications; critical infrastructure owner/operators; and analyst consuming communications assessments.

The Emergency Response Operations (ERO) Branch Feedback Form consists of five customer surveys:

- *Emergency Response Operations Communications Analysis Survey Feedback Form.*
- *Emergency Support Function (ESF) #2 Survey Feedback Form.*
- *Emergency Support Function #14 Survey Feedback Form.*
- *ERO National Coordinating Center for Communications (NCC) - Information Sharing and Analysis Center (ISAC) Survey Feedback Form.*
- *National Security Emergency Preparedness (NSEP) Continuity Survey Feedback Form.*

Analyzing feedback from stakeholders was recently identified as a recommendation in a Government Accountability Office (GAO) Audit. A link will be provided to the various distribution lists through Microsoft Forms.

As required under the Paperwork Reduction Act (PRA), this Privacy Threshold Analysis is being completed because the survey forms, once approved by OMB, will collect feedback from the public to assess the utility of CISA Central/ERO products in order to guide and improve future products and processes. The feedback will include the collection of a limited amount of personal identifiable information (PII) for the purposes of further communication between SLTT respondents, industry private sector partners and CISA Central/ERO for any necessary clarification of the feedback given.



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.*

The creation of a feedback survey available to stakeholders is in response to a recommendation recently identified in a Government Accountability Office (GAO) Report 22-104462- [GAO-22-104462](#) Critical Infrastructure Protection: CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector. Therefore, CISA Central will collect, store, and use this information.

2. Describe the IC/Form	
a. Does this form collect any Personally Identifiable Information” (PII ¹)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
b. From which type(s) of individuals does this form collect information? <i>(Check all that apply.)</i>	<input checked="" type="checkbox"/> Members of the public <ul style="list-style-type: none"> <input checked="" type="checkbox"/> U.S. citizens or lawful permanent residents <input checked="" type="checkbox"/> Non-U.S. Persons. <input checked="" type="checkbox"/> DHS Employees <input checked="" type="checkbox"/> DHS Contractors <input checked="" type="checkbox"/> Other federal employees or contractors.
c. Who will complete and submit this form? <i>(Check all that apply.)</i>	<input checked="" type="checkbox"/> The record subject of the form (e.g., the individual applicant). <input type="checkbox"/> Legal Representative (preparer, attorney, etc.). <input type="checkbox"/> Business entity. If a business entity, is the only information collected business contact information? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Law enforcement.

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.



	<input type="checkbox"/> DHS employee or contractor. <input type="checkbox"/> Other individual/entity/organization that is NOT the record subject. <i>Please describe.</i>										
<p>d. How do individuals complete the form? <i>Check all that apply.</i></p>	<input type="checkbox"/> Paper. <input type="checkbox"/> Electronic. (ex: fillable PDF) <input checked="" type="checkbox"/> Online web form. (available and submitted via the internet) <i>Provide link:</i> https://forms.office.com/g/da1g6u6QDN https://forms.office.com/g/3SykS8diuy https://forms.office.com/g/hJ3HJ7k55J https://forms.office.com/g/NAwpqxLR7x https://forms.office.com/g/h2KzU0FmRL										
<p>e. What information will DHS collect on the form? <i>List all 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></p>											
<p>The surveys are designed capture stakeholder feedback on shared products to ensure value to recipients and to guide and improve future products and processes. In the survey, CISA Central/ERO is asking internal and external partners for the usefulness and satisfaction of the products that we send. This survey collection allows stakeholders to provide their email as optional should further clarification be needed.</p> <p>Email address is the only form of personally identifiable information to be collected on the survey form.</p>											
<p>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> Not Applicable</p>											
<table border="0"> <tr> <td><input type="checkbox"/> Social Security number</td> <td><input type="checkbox"/> DHS Electronic Data Interchange</td> </tr> <tr> <td><input type="checkbox"/> Alien Number (A-Number)</td> <td>Personal Identifier (EDIPI)</td> </tr> <tr> <td><input type="checkbox"/> Tax Identification Number</td> <td><input type="checkbox"/> Social Media Handle/ID</td> </tr> <tr> <td><input type="checkbox"/> Visa Number</td> <td><input type="checkbox"/> Known Traveler Number</td> </tr> <tr> <td><input type="checkbox"/> Passport Number</td> <td></td> </tr> </table>		<input type="checkbox"/> Social Security number	<input type="checkbox"/> DHS Electronic Data Interchange	<input type="checkbox"/> Alien Number (A-Number)	Personal Identifier (EDIPI)	<input type="checkbox"/> Tax Identification Number	<input type="checkbox"/> Social Media Handle/ID	<input type="checkbox"/> Visa Number	<input type="checkbox"/> Known Traveler Number	<input type="checkbox"/> Passport Number	
<input type="checkbox"/> Social Security number	<input type="checkbox"/> DHS Electronic Data Interchange										
<input type="checkbox"/> Alien Number (A-Number)	Personal Identifier (EDIPI)										
<input type="checkbox"/> Tax Identification Number	<input type="checkbox"/> Social Media Handle/ID										
<input type="checkbox"/> Visa Number	<input type="checkbox"/> Known Traveler Number										
<input type="checkbox"/> Passport Number											



<input type="checkbox"/> Bank Account, Credit Card, or other financial account number	<input type="checkbox"/> Trusted Traveler Number (Global Entry, Pre-Check, etc.)
<input type="checkbox"/> Other. <i>Please list:</i>	<input type="checkbox"/> Driver's License Number
	<input type="checkbox"/> Biometrics

g. List the **specific authority** to collect SSN or these other SPII elements.

Not Applicable

h. How will this information be used? What is the purpose of the collection? Describe **why** this collection of SPII is the minimum amount of information necessary to accomplish the purpose of the program.

The purpose of the surveys is to capture stakeholder feedback on shared products to ensure value to recipients and to guide and improve future products and processes. This collection does not contain SPII.

i. 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>)?	<input checked="" type="checkbox"/> Yes. Please describe how notice is provided. Prior to the forms being approved by OMB and the PRA Office, CISA Central/ERO will notify internal and external partners of a voluntary survey attached to the different products submitted. A Privacy Act statement will be at the bottom of each form notifying each respondent of the collection and use of information by CISA Central/ERO. <input type="checkbox"/> No.
---	---

3. How will DHS store the IC/form responses?

a. How will DHS store the original, completed IC/forms?	<input type="checkbox"/> Paper. Please describe. Click here to enter text. <input checked="" type="checkbox"/> Electronic. Please describe the IT system that will store the data from the form. The survey will be stored online in CISA Microsoft's cloud servers. CISA Central Standards and Evaluations Team will have the sole authority to grant access to the survey and its responses in individuals within CISA Central/ERO who have an official need to know.
---	--



	<input type="checkbox"/> 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>	<input type="checkbox"/> Manually (data elements manually entered). Please describe. Click here to enter text. <input checked="" type="checkbox"/> Automatically. Please describe. The Stakeholder inputs their responses into Microsoft Forms. Once the survey has been completed, the responses remain in the forms where they are reviewed by CISA Central/ERO
<p>c. How would a user search the information submitted on the forms, <i>i.e.</i>, how is the information retrieved?</p>	<input checked="" type="checkbox"/> By a unique identifier. ² <i>Please describe.</i> If information is retrieved by personal identifier, please submit a Privacy Act Statement with this PTA. Respondents email address <input checked="" type="checkbox"/> By a non-personal identifier. <i>Please describe.</i> Partner Type, title of report, and date of report/product
<p>d. What is the records retention schedule(s)? <i>Include the records schedule number.</i></p>	The information collected by CISA/ERO will be retained in accordance with the following schedule, DAA-GRS-20170001-0001 Item 010 - <u>Technical and Administrative Help Desk Operational Records</u>
<p>e. How do you ensure that records are disposed of or deleted in accordance with the retention schedule?</p>	In accordance with DAA-GRS-20170001-0001 Item 010, records are to be destroyed 1 year after resolved, or when no longer needed for business use, whichever is appropriate.

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.



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>	
<input type="checkbox"/> Yes, information is shared with other DHS components or offices. Please describe. Click here to enter text.	
<input type="checkbox"/> 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.	
<input checked="" type="checkbox"/> 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:	Cassio DaCunha
Date submitted to component Privacy Office:	March 11, 2022
Date submitted to DHS Privacy Office:	March 25, 2022
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>	<input type="checkbox"/> Yes. Please include it with this PTA submission. <input type="checkbox"/> No. Please describe why not. Click here to enter text.
<p>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></p> <p>CISA Central’s Emergency Response Operations (ERO) interacts with a variety of stakeholders across multiple mission areas to support regional and national disasters, supports Continuity and National Security Emergency Preparedness, and serve as the Communications Information Sharing and Analysis Center. The purpose of the feedback form is to capture stakeholder feedback on shared products to ensure value to recipients and to guide and improve future products and processes.</p> <p>The CISA Office of Privacy recommends that the use of the CISA Central ERO Stakeholder Feedback Form is privacy sensitive due to its collection of personally identifiable information and is covered by DHS/ALL/PIA – 006 DHS General Contacts List and DHS/ALL/PIA-069 DHS Surveys, Interviews, and Focus Groups. The PII collected is also covered under DHS/ALL – 002 Department of Homeland Security (DHS) Mailing and Other Lists System November 25, 2008, 73 FR 71659.</p>	



PRIVACY THRESHOLD ADJUDICATION

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	Kattina Do
PCTS Workflow Number:	0022189
Date approved by DHS Privacy Office:	March 25, 2022
PTA Expiration Date	March 25, 2025

DESIGNATION

Privacy Sensitive IC or Form:	Yes If "no" PTA adjudication is complete.
Determination:	<input type="checkbox"/> PTA sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing SPII applies. <input checked="" type="checkbox"/> Privacy Act Statement required. <input checked="" type="checkbox"/> Privacy Impact Assessment (PIA) required. <input checked="" type="checkbox"/> System of Records Notice (SORN) required. <input type="checkbox"/> Specialized training required. <input type="checkbox"/> Other. Click here to enter text.
DHS IC/Forms Review:	DHS PRIV has approved this ICR/Form.
Date IC/Form Approved by PRIV:	March 25, 2022
IC/Form PCTS Number:	Emergency Response Operations Stakeholder Feedback Form
Privacy Act Statement:	Choose an item. Click here to enter text.
PTA:	Choose an item. Click here to enter text.
PIA:	System covered by existing PIA If covered by existing PIA, please list:



	<ul style="list-style-type: none"> • DHS/ALL/PIA-069 DHS Surveys, Interviews, and Focus Groups • DHS/ALL/PIA-006 General Contact Lists <p>If a PIA update is required, please list: Click here to enter text.</p>
SORN:	<p>System covered by existing SORN</p> <p>If covered by existing SORN, please list:</p> <ul style="list-style-type: none"> • DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, November 25, 2008, 73 FR 71659 <p>If a SORN update is required, please list: Click here to enter text.</p>
<p>DHS Privacy Office Comments: <i>Please describe rationale for privacy compliance determination above.</i></p>	
<p>CISA is submitting this PTA to discuss the Emergency Response Operations Stakeholder Feedback Form. CISA Central is CISA's hub for staying on top of threats and emerging risks to our nation's critical infrastructure, whether they are of cyber, communications or physical origin.</p> <p>Within CISA Central, the Emergency Response Operations (ERO) Branch performs emergency support functions to support CISA's roles as the Emergency Support Function (ESF) Coordinator and Co-Primary Agency (along with FEMA) to support regional and national disasters, supports Continuity and National Security Emergency Preparedness, and serves as the Communications Information Sharing and Analysis Center (ISAC).</p> <p>CISA Central's ERO interacts with a variety of stakeholders across multiple mission areas. The purpose of the surveys is to capture stakeholder feedback on shared products to ensure value to recipients and to guide and improve future products and processes.</p> <p>The Emergency Response Operations (ERO) Branch Feedback Form consists of five customer surveys.</p> <ol style="list-style-type: none"> 1. Emergency Response Operations Communications Analysis Survey Feedback Form. 2. Emergency Support Function (ESF) #2 Survey Feedback Form. 3. Emergency Support Function #14 Survey Feedback Form. 4. ERO National Coordinating Center for Communications (NCC) - Information Sharing and Analysis Center (ISAC) Survey Feedback Form. 5. National Security Emergency Preparedness (NSEP) Continuity Survey Feedback Form. <p>Analyzing feedback from stakeholders was recently identified as a recommendation in a Government Accountability Office (GAO) Audit. A link will be provided to the various distribution lists through Microsoft Forms.</p>	



The surveys are designed capture stakeholder feedback on shared products to ensure value to recipients and to guide and improve future products and processes. In the survey, CISA Central/ERO is asking internal and external partners for the usefulness and satisfaction of the products that we send. This survey collection allows stakeholders to provide their email as optional should further clarification be needed. Email address is the only form of personally identifiable information to be collected on the survey form.

The DHS Privacy Office (PRIV) agrees that this form is privacy-sensitive, requiring PIA and SORN coverage because PII is collected from members of the public, DHS personnel, and other federal employees.

PRIV agrees with CISA Privacy that PIA coverage is provided by DHS/ALL/PIA-069 DHS Surveys, Interviews, and Focus Groups provides transparency into the privacy risks associated with DHS's collection, maintenance, and use of PII in order to facilitate correspondence via a survey. Additionally, 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 personal identifier. PRIV agrees with CISA Privacy that 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.

CISA is required to update and use the Privacy Act Statement attached to this PTA. Also, any updates to this form will require an update to this PTA.