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

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

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:	**Active Exploitation Reporting Submission Form**		
Component:	Cybersecurity and Infrastructure Security Agency (CISA)	Office:	Cybersecurity Division (CSD), Vulnerability Management (VM)

IF COVERED BY THE PAPERWORK REDUCTION ACT:

Collection Title:	**Click here to enter text.**		
OMB Control Number:	Click here to enter text.	OMB Expiration Date:	Click here to enter a date.
Collection status:	Choose an item.	Date of last PTA (if applicable):	Click here to enter a date.

PROJECT OR PROGRAM MANAGER

Name:	Christopher Murray		
Office:	CSD / VM	Title:	IT Specialist
Phone:	Click here to enter text.	Email:	Christopher.Murray@cisa.dhs.gov

COMPONENT INFORMATION COLLECTION/FORMS CONTACT

Name:	Click here to enter text.		
Office:	Click here to enter text.	Title:	Click here to enter text.
Phone:	Click here to enter text.	Email:	Click here to enter text.

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 Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Division (CSD) Vulnerability Management (VM) subdivision is submitting this updated PTA for the Active Exploitation Reporting Submission Form, which was previously adjudicated in December 2021. Since the last adjudication, the program manager for this effort has changed and the form itself has yet to be published. The form is expected to go live once this Privacy Threshold Analysis (PTA) has been adjudicated and the Paperwork Reduction Act (PRA) package has been approved by the Office of Management and Budget (OMB).

CISA's cybersecurity mission is to defend and secure cyberspace by leading national efforts to drive and enable effective national cyber defense, resilience of national critical functions, and a robust technology ecosystem.[1] To do that, CSD and its subdivisions have devised ample programs and resources to defend against immediate threats and vulnerabilities. VM specifically focuses on reducing the prevalence and impact of vulnerabilities and exploitable conditions across enterprises and technologies, including through assessments and coordinated disclosure of vulnerabilities by trusted partners.[2]

One such VM-led effort seeks to leverage the cybersecurity community to help track active exploitations in the public domain. The Active Exploitation Reporting Submission Form will broaden CISA's scope of known and exploited vulnerabilities, benefiting not only the agency but the cybersecurity posture of our partners and stakeholders as well. Presently, individuals are able to call or email CISA Central[3] to report any new or actively exploited vulnerabilities. The form will be made publicly available on CISA.gov and will present an alternative to the aforementioned reporting options.

Once publicly available, completed forms will be submitted electronically through CISA.gov and auto forwarded to an Outlook mailbox managed by VM. Upon receipt,

[1] https://www.cisa.gov/about/divisions-offices/cybersecurity-division.
[2] https://www.cisa.gov/vulnerability-management.
[3] https://www.cisa.gov/cisa-central.

submission forms are entered as service tickets in ServiceNow for further review and analysis. When completing the form, individuals are provided the opportunity to voluntarily include their contact information along with the submission form. CISA will use the contact information to collect additional information as needed about the active exploitation report. Contact information will not be used for any other purpose than follow-up, and information will not be retrieved by personal identifier.
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, 659, and 44 U.S.C § 3101 authorize the collection of this information.

2. Describe the IC/Form	
a. Does this form collect any Personally Identifiable Information" (PII[4])?	☒ 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 (list Components): Any/All ☒ 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

[4] 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.

	☐ No ☐ Law enforcement. ☐ DHS employee/contractor. ☐ Other individual/entity/organization **that is NOT the record subject**. *Please describe*.
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:* https://www.cisa.gov/forms/kev [5]
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.*	
The Reporting Submission Form collects the following exploitation-specific information from users: **1) Common Vulnerabilities and Exposures (CVE) ID[6]** **2) Patch or Clear Mitigation Guidance** **3) Exploitation Evidence** **Users are not required to provide any personally identifiable information in order for their report to be successfully submitted, however the opportunity to provide contact information is provided to users on a voluntary basis. This includes full name and email address.**	
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 ☐ Alien Number (A-Number) ☐ Tax Identification Number ☐ Visa Number ☐ Passport Number	☐ 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

[5] This link will "go live" only after the PTA has been successfully adjudicated by DHS Privacy and the PRA package approved by the Office of Management and Budget (OMB).
[6] *See* CISA's Known Exploited Vulnerabilities Catalog, available at https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

☐ Bank Account, Credit Card, or other financial account number ☐ Other. *Please list:*	☐ 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? *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.	
N/A	
j. Are individuals provided notice at the time of collection by DHS (*Does the records subject have notice of the collection or is form filled out by third party*)?	☒ Yes. Please describe how notice is provided. **Notice is provided via Privacy Act Statement in advance of the reporting submission form.** ☐ No.

3. How will DHS store the IC/form responses?	
a. How will DHS store the original, completed IC/forms?	☐ Paper. Please describe. Click here to enter text. ☒ Electronic. Please describe the IT system that will store the data from the form. **Completed forms are sent directly to an Outlook mailbox owned and operated by the program. Following receipt, a ticket is registered in ServiceNow to ensure the active exploitation is tracked and recorded.**

	☐ Scanned forms (completed forms are scanned into an electronic repository). Please describe.
b. If electronic, how does DHS input the responses into the IT system?	☐ Manually (data elements manually entered). Please describe. ☒ Automatically. Please describe. **Electronic submission forms are automatically sent to a designated Outlook mailbox then registered in ServiceNow as a ticket for action.**
c. How would a user search the information submitted on the forms, *i.e.*, how is the information retrieved?	☐ By a unique identifier.[7] *Please describe*. If information is retrieved by personal identifier, please submit a Privacy Act Statement with this PTA. ☒ By a non-personal identifier. *Please describe*. **Information will be retrieved by ticket number or CVE-ID.**
d. What is the records retention schedule(s)? *Include the records schedule number.*	**General Record Schedule (GRS) 3.2 item 020** Information System Security Records: Computer security incident handling, reporting and follow up records.
e. How do you ensure that records are disposed of or deleted in accordance with the retention schedule?	**Temporary.** Destroy 3 year(s) after all necessary follow-up actions have been completed, but longer retention is authorized if required for business use.
f. Is any of this information shared outside of the original program/office? *If yes, describe where (other offices or DHS components or external entities) and why. What are the authorities of the receiving party?*	
☐ Yes, information is shared with other DHS components or offices. Please describe. Click here to enter text.	

[7] 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 *external* 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.

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

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

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	**Donna Hellberg**
Date submitted to Component Privacy Office:	Click here to enter a date.
Concurrence from other Components involved (if applicable):	Click here to enter text.
Date submitted to DHS Privacy Office:	January 30, 2025
Have you approved a Privacy Act Statement for this form? (*Only applicable if you have received a waiver from the DHS Chief Privacy Officer to approve component Privacy Act Statements.*)	☒ Yes. Please include it with this PTA submission. ☐ No. Please describe why not. Click here to enter text.

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

CISA's Office of Privacy, Access, Civil Liberties and Transparency (PACT) is submitting this updated PTA on behalf of the Cybersecurity Division (CSD), Vulnerability Management (VM) subdivision for their Active Exploitation Reporting Submission Form. Since the last adjudication, the program manager for this effort has changed. Additionally, the form described in the initial PTA for this effort was never published – and as a result, no records were collected or stored in connection with this form.

In addition to vulnerability, exploitation and exposure information, the form permits individuals to voluntarily provide their contact information for follow-up by CISA as needed. PACT therefore recommends that the collection is privacy sensitive requiring PIA coverage.

PIA coverage is provided by DHS/ALL/PIA-069 DHS Surveys, Interviews, and Focus Groups, which permits DHS and its components to periodically solicit input from its employees, contractors, external stakeholders, and the public to improve DHS services and operations. Additional PIA coverage is provided by DHS/ALL/PIA-006 General Contacts List, which covers the collection of contact information for the purpose of conducting agency operations.

SORN coverage is not required as information is not retrieved by unique identifier.

Active Exploitation Reporting Submission Form
Privacy Act Statement

Authorities: 6 U.S.C. §§ 652, 659, and 44 U.S.C § 3101 authorize the collection of this information.

Purpose: The purpose of this collection is to solicit and receive voluntary submissions of active exploitations from the general public for awareness, tracking and notification purposes**.**

Routine Uses: This information may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes using information, as necessary and authorized by DHS/ALL/PIA-069 DHS Surveys, Interviews, and Focus Groups, which permits DHS and its components to periodically solicit input from its employees, contractors, external stakeholders, and the public to improve DHS services and operations. Additional PIA coverage is provided by DHS/ALL/PIA-006 General Contacts List, which covers the collection of contact information for the purpose of conducting agency operations. Providing contact information when reporting an active exploitation is optional; if provided, CISA will only use this information to contact the reporter with questions relating to their submission.

Disclosure: Providing this information is voluntary; however, failure to provide this information may prevent the individual from receiving follow-up communications about their submission.

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

PRIVACY THRESHOLD ADJUDICATION

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	**Sean McGuinness**
PRIVCATS Workflow Number:	**0018909**
Date approved by DHS Privacy Office:	**February 11, 2025**
PTA Expiration Date	**February 11, 2028**
DHS Privacy Office Approver (if applicable):	Click here to enter text.

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:	Choose an item. **The Privacy Act Statement attached to the PTA submission is 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-069 DHS Surveys, Interviews, and Focus Groups; and** • **DHS/ALL/PIA-006 General Contacts Lists.**

	If a PIA update is required, please list: Click here to enter text.
SORN:	If covered by existing SORN, please list: Click here to enter text. If a SORN update is required, please list: Click here to enter text.

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

CISA is submitting this PTA to document the renewal of the Active Exploitation Reporting Submission. The Active Exploitation Reporting Submission Form will be publicly available for individuals to complete and provide information on the active exploitation of known vulnerabilities. CISA works closely with the cybersecurity community to track active exploitation in the public domain. By collecting and aggregating this data, CISA will be able to not only track new reports of active exploitation but to share this information with our trusted stakeholders. Contact information of the individual reporting the active exploitation will be optional and only used by CISA to contact the individual with questions related to their submission.

The DHS Privacy Office (PRIV) finds that the Active Exploitation Reporting Submission Form is privacy sensitive as it collects PII from members of the public and DHS employees/contractors.

PRIV agrees with CISA Privacy that PIA coverage is provided by:

- **DHS/ALL/PIA-069 DHS Surveys, Interviews, and Focus Groups, which permits DHS and its components to periodically solicit input from its employees, contractors, external stakeholders, and the public to improve DHS services and operations; and**
- **DHS/ALL/PIA-006 General Contacts Lists, which covers the collection of contact information for the purpose of conducting agency operations.**

PRIV finds that SORN coverage is not required as information is not retrieved by personal identifier.

The Privacy Act Statement attached to this PTA submission is approved.