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:	**11000-39**		
Form Title:	**CISA Visitor Request Form**		
Component:	Cybersecurity and Infrastructure Security Agency (CISA)	Office:	**Office of the Chief Compliance and Security Officer**

IF COVERED BY THE PAPERWORK REDUCTION ACT:

Collection Title:	**CISA Visitor Request Form**		
OMB Control Number:	1670-0036	OMB Expiration Date:	TBD
Collection status:	Extension	Date of last PTA (if applicable):	**October 21, 2019**

PROJECT OR PROGRAM MANAGER

Name:	Michael Washington		
Office:	Office of the Chief Compliance and Security Officer	Title:	Security Specialist
Phone:	703-235-1925	Email:	Michael.Washington@cisa.dhs.gov

COMPONENT INFORMATION COLLECTION/FORMS CONTACT

Name:	Mia Bruce		
Office:	Office of the Chief Information Officer	Title:	PRA Program Coordinator
Phone:	202-713-6210	Email:	Mia.Bruce@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.

The Office of the Chief Compliance and Security (OCSO) Officer within the Cybersecurity and Infrastructure Security Agency (CISA) will submit the following renewal CISA Visitor Request Form PTA. Information Public Law 107-296 and The Homeland Security Act of 2002, Title II, recognizes the Department of Homeland Security role in integrate relevant critical infrastructure and cybersecurity information, analyses, and vulnerability assessments (whether such information, analyses, or assessments are provided or produced by the Department or others) in order to identify priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local government agencies and authorities, the private sector, and other entities while maintaining positive control of sensitive information regarding the national infrastructure. In support of this mission the Cybersecurity and Infrastructure Security Agency Office of the Chief Compliance and Security Officer must maintain a robust visitor screening capability.

The Office of Compliance and Security will only use electronic submission via email of the collection information using an electronic fillable pdf form. This decision allows for the efficient collection of information about visits, with minimal cost to the government. The form is requested by CISA employees or contractors to complete for non-DHS guests visiting CISA facilities. The form is available via the internal DHS website or by requesting a copy of the form from the Office of Compliance and Security.

The purpose of this form is to allow security officers to conduct a risk-based pre-screening of visitors to CISA facilities in accordance with DHS and GSA requirements to pre-screen and register visitors.

The CISA Visitor Request Form must be completed and submitted to the Office of the Chief Compliance and Security Officer (OCSO) by a current DHS Headquarters employee or contractor that is serving as the requestor for the visitor(s) in question.

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.*
5 U.S.C. 301; the Homeland Security Act, codified in Title 6 of the U.S. Code; 44 U.S.C. 3101; and Executive Order (EO) 9397; EO 12968; and Federal Property Regulations, issued July 2002, authorize the collection of this information. DHS 121-01-011-01 and 41 CFR parts 102-74 require that visitors to are pre-screened and registered.

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 ☒ DHS Contractors ☒ 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 or contractor.

[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.

	☐ 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:*

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

Name and phone number of requestor; Name and phone number of point of contact (if different from requestor); Name and phone number of escort (if different from requestor); Visitor name, organization, and in some cases the last four digits of visitors' Social Security number (For Classified Meetings only).

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 Personal Identifier (EDIPI)
☐ Alien Number (A-Number)	☐ Social Media Handle/ID
☐ Tax Identification Number	☐ Known Traveler Number
☐ Visa Number	☐ Trusted Traveler Number (Global Entry, Pre-Check, etc.)
☐ Passport Number	☐ Driver's License Number
☐ Bank Account, Credit Card, or other financial account number	☐ Biometrics
x Other. *Please list: Last Four of SSN for Classified Meetings*	

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

Executive Order (EO) 9397 authorizes the collection of this information.

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.	
Use is 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 the routine uses published in DHS/ALL-024 Facility and Perimeter Access Control Management System of Records. Security Officers will use this information to positively identify an individual and make a risk-based decision to allow entry to an CISA facility. The last four digits of an individual's SSN, only collected for classified visits, is used to make positive identification of an individual in order to verify his or her security clearance(s).	
i. 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. **There is a Privacy Act Notice included on the form providing notice to the requestor.** ☐ No.

3. How will DHS store the IC/form responses?	
a. How will DHS store the original, completed IC/forms?	☒ Paper. Please describe. **Forms are printed and stored for thirty days, and are then destroyed** ☒ Electronic. Please describe the IT system that will store the data from the form. **Name, Organization, Date of Visit and Escort Name and Phone number are stored in a spreadsheet, located on an SPII approved SharePoint site with limited access, for 3 years (SSN is not recorded)** ☐ 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. **Data is manually added to the excel spreadsheet, SSN is not recorded** ☐ Automatically. Please describe. Click here to enter text.
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. **Users may search using name or date of visit** ☐ By a non-personal identifier. *Please describe*. Click here to enter text.
d. What is the records retention schedule(s)? *Include the records schedule number.*	**These records are managed as *Visitor Control Files* under General Records Schedule (GRS) 18, 1960, item 18.**
e. How do you ensure that records are disposed of or deleted in accordance with the retention schedule?	**As *Visitor Control Files* under GRS 18, the visitor logs will be retained until such time as they are destroyed:** **• 5 years after final entry or date of document for areas under maximum security; or** **• 2 years after final entry or date of document for other areas.**
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. ☐ 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.	

[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.

☒ 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 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:	**Cheryl Dyson-Bennett/Scherida Lambert**
Date submitted to component Privacy Office:	**November 25, 2020**
Date submitted to DHS Privacy Office:	December 4, 2020
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.*	
The Office of the Chief Privacy Officer has reviewed and determined this to be a privacy sensitive collection that is covered by DHS/ALL-024 Facility and Perimeter Access Control Management System of Records and DHS/ALL/PIA – 038 – Integrated Security Management System (ISMS).	

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:	**Kattina Do**
DHS Privacy Office Approver (if applicable):	Max Binstock
PCTS Workflow Number:	**0015455**
Date approved by DHS Privacy Office:	December 4, 2020
PTA Expiration Date	December 4, 2023

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.
DHS IC/Forms Review:	DHS PRIV has approved this ICR/Form.
Date IC/Form Approved by PRIV:	December 4, 2020
IC/Form PCTS Number:	**Form 11000-39**
Privacy Act Statement:	**e(3) statement update is required.** 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: • DHS/ALL/PIA-039 Physical Access Control System (PACS) 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-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management February 3, 2010, 75 FR 5609 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 renewal PTA to discuss the CISA Visitor Request Form. NPPD is now CISA. The purpose of this form is to allow security officers to conduct a risk-based pre-screening of visitors to CISA facilities in accordance with DHS and GSA requirements to pre-screen and register visitors.

The form is requested by CISA employees or contractors to complete for non-DHS guests visiting CISA facilities. The form is available via the internal DHS website or by requesting a copy of the form from the Office of Compliance and Security. The Office of Compliance and Security will only use electronic submission via email of the collection information using an electronic fillable pdf form.

The form will collect name and phone number of requestor; name and phone number of point of contact (if different from requestor); name and phone number of escort (if different from requestor); visitor name, organization, and in some cases the last four digits of visitors' Social Security number (For Classified Meetings only).

The DHS Privacy Office (PRIV) finds that this form is privacy-sensitive, and a PIA is required because PII is collected from members of the public, DHS Employees, DHS contractors, and other federal employees or contractors.

PRIV disagrees with CISA Privacy that DHS/ALL/PIA-038 ISMS PIA provides coverage because CISA does not share this information with ISMS. PIA coverage is provided by DHS/ALL/PIA-039 Physical Access Control System (PACS), which covers the use of the range of functions related to managing physical access by individuals to DHS

facilities. PACS are generally comprised of four major functions: visitor management, physical access control, intrusion detection, and video surveillance.

PRIV agrees with CISA Privacy that a SORN is required because info is being retrieved by a unique identifier. PRIV agrees with CISA Privacy and finds that SORN coverage is provided by DHS/ALL-024 Facility and Perimeter Access Control and Visitor Management, which covers the collection of records related to the Department's facility and perimeter access control, including access to DHS information technology and access to classified facilities, as well as visitor security and management.

CISA has also submitted a sufficient Privacy Act Statement with this PTA.