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 will be used to determine whether a Privacy Impact Assessment (PIA), System of Records Notice (SORN), or other privacy compliance documentation is required under the E-Government Act of 2002, the Homeland Security Act of 2002, the Privacy Act of 1974, or U.S. Department of Homeland Security (DHS) policy.

Please complete this form and send it to your Component Privacy Office. If you are unsure of your Component Privacy Office contact information, please visit https://www.dhs.gov/privacy-office-contacts. If you do not have a Component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
DHS Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717

PIA@hq.dhs.gov

Your Component Privacy Office will submit the PTA on behalf of your office. Upon receipt from your Component Privacy Office, the DHS Privacy Office will review this form. If a PIA, SORN, or other privacy compliance documentation is required, your Component Privacy Office, in consultation with the DHS Privacy Office, will send you a copy of the template to complete and return.

For more information about the DHS Privacy compliance process, please see https://www.dhs.gov/compliance. A copy of the template is available on DHS Connect at http://dhsconnect.dhs.gov/org/offices/priv/Pages/Privacy-Compliance.aspx or directly from the DHS Privacy Office via email: PIA@hq.dhs.gov or phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project, Program, or System Name:	**.gov Top-Level Domain (TLD) Program**		
Component or Office:	Cybersecurity and Infrastructure Security Agency (CISA)	**Office or Program:**	Cybersecurity Division (CSD) Capacity Building (CB)
FISMA Name (if applicable):	N/A	**FISMA Number (if applicable):**	N/A
Type of Project or Program:	Program	**Project or program status:**	Operational
Date first developed:	June 17, 2020	**Pilot launch date:**	N/A
Date of last PTA update	February 11, 2021	**Pilot end date:**	N/A
ATO Status (if applicable):[1]	N/A	**Expected ATO/ATP/OA date (if applicable):**	N/A

PROJECT, PROGRAM, OR SYSTEM MANAGER

Name:	**Cameron Dixon**		
Office:	CSD Capacity Building	**Title:**	Policy technologist
Phone:	(202) 631-0602	**Email:**	cameron.dixon@cisa.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	**Cameron Dixon**		
Phone:	(202) 631-0602	**Email:**	cameron.dixon@cisa.dhs.gov

[1] The DHS OCIO has implemented a streamlined approach to authorizing an Authority to Operate (ATO), allowing for rapid deployment of new IT systems and initiate using the latest technologies as quickly as possible. This approach is used for selected information systems that meet the required eligibility criteria in order to be operational and connect to the network. For more information, see http://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/CISO%20ALL%20Documents/Authority%20to%20Proceed%20Memo%20Phase%20II.pdf.

1. Reason for submitting the PTA: Updated PTA

This Updated PTA documents the information sharing between the Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Division (CSD) Capacity Building (CB) and the U.S. Census Bureau in connection with CISA's administration of the .gov Top-Level Domain (TLD) program. Information, including personally identifiable information, related to U.S.-based government organizations is shared pursuant to a Memorandum of Agreement (MOA) between CISA and the Census Bureau. No operational changes have been made to the program since the previous PTA adjudication. The program name provided on this PTA has been changed from ".gov TLD registry and registrar" to ".gov Top Level Domain (TLD) Program".

The Domain Name System (DNS) is the internet service that translates between the *names humans prefer* and the *numbers computers need* to navigate to a website or send an email address. Those names, called "domain names" are registered by an entity for their internet brand on websites, emails, or other online services affiliated with the entity. "dhs.gov" is an example of the U.S. Department of Homeland Security's primary domain name, and .gov is one of many "top-level domains"; others include .com, .org, and .edu. Each TLD is managed by a registry operator which controls what domain names can be registered and how.

The DOTGOV Online Trust in Government Act of 2020 transferred responsibility for the .gov TLD from the General Services Administration (GSA) to CISA. As the registry operator of the .gov TLD, CISA (through its contracted entity) manages the .gov registry and the .gov registrar. The .gov registry is the DNS infrastructure that makes the TLD and all registered .gov domain names available over the internet. The .gov registrar is the web application where users register and manage .gov domain names. CISA also oversees the security of the .gov namespace and facilitates reporting of potential security incidents to registrants.

<u>.gov Registration</u>

After confirming that the domain name they are requesting is available, a government organization submits an authorization letter to CISA. Authorization letters include the name of the authorizing authority, administrative contact, technical contact and each associated physical address and phone number. The authorization letters may also contain citations or additional information about the organization's status as a government. CISA uses the information provided in this letter to establish if the organization is eligible for a .gov domain, if the request is from the appropriate authority within the organization and if the person making the request is actually that authority. Verification uses multiple sources, including information from the Census Bureau's census of governments.[2]

Once identity verification has occurred, a .gov registrar account is created for each contact for the domain. These individuals are given user-level access to the registrar and can then login using a government-defined username and a user-set password. After each domain contact has logged in to establish their account, any of these individuals may complete the online domain request form. This form collects information similar to what was initially provided in the authorization letter. After the online

[2] *See https://www.census.gov/library/publications/2019/econ/2017isd.html*

domain request form is completed, the request undergoes final review. If approved, the request is complete when the new domains are put online by being entered into the .gov zone file.

CISA contracts with a vendor to operate the technical infrastructure that comprise the .gov domain registry and registrar. The systems are housed at a contracted site and managed at data centers with physical access control.

Census Bureau and CISA Information Sharing Project

As administrator of the .gov TLD program, CISA evaluates and authorizes requests for .gov domains using various government and commercial information sources to ensure that requests for .gov domains are granted only to legitimate government organizations and officials.

One source of information is the Census Bureau, which maintains and updates information regarding all state and local governments in the United States within several databases and Information Technology systems. Specific data types that assist the .gov TLD program in assessing the legitimacy of a .gov domain request includes location, type and characteristics of all state and local governments in the United States, as well as contact information, including names, departments, position/title information, phone numbers and email addresses.

In the joint sharing project, CISA and the Census Bureau will share relevant data about U.S.-based government organizations and collaborate to resolve potential discrepancies, to improve the accuracy and relevance of the information, thereby enabling both organizations to fulfill their missions more effectively.

The OCPO and the .gov TLD Program, with input and review from CISA's Office of the Chief Counsel (OCC), have drafted a Privacy Act Statement (included in the Component Privacy Office Recommendation section below) that will be displayed on the .gov registration page. We have also drafted a Privacy Notice that will be displayed on the authorization letter template page. This Privacy Notice will provide registrants with notice that CISA will share approved authorization letters submitted by the authorizing authority requesting a .gov domain with the Census Bureau, including letters that have already been collected by CISA.

2. From whom does the Project, Program, or System collect, maintain, use, or disseminate information? *Please check all that apply.*	☐ This project does not collect, collect, maintain, use, or disseminate any personally identifiable information[3] ☒ Members of the public

[3] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that 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. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

	☒ U.S. Persons (U.S citizens or lawful permanent residents) – Officials from U.S.-based government organizations. ☐ Non-U.S. Persons ☒ DHS Employees/Contractors (list Components): A contracted entity (currently VeriSign Inc.) ☒ Other federal employees or contractors (list agencies): Officials from U.S.-based government organizations.
2(a) Is information meant to be collected from or about sensitive/protected populations?	☒ No ☐ 8 USC § 1367 protected individuals (e.g., T, U, VAWA)[4] ☐ Refugees/Asylees ☐ Other. Please list: *Click here to enter text.*

3. What specific information about individuals is collected, maintained, used, or disseminated?

.gov Registration

U.S.-based government organizations requesting a .gov domain address must provide contact information including first name, last name, governmental organization phone number, email address, and mailing address.

Census Bureau and CISA Information Sharing Project

Specific information about individuals CISA will disseminate to the Census Bureau:

- Name of the authorizing authority, administrative contact, technical contact and security contact
- Physical addresses
- Email addresses

[4] This involves the following types of individuals: T nonimmigrant status (Victims of Human Trafficking), U nonimmigrant status (Victims of Criminal Activity), or Violence Against Women Act (VAWA). For more information about 1367 populations, please see: DHS Management Directive 002-02, Implementation of Section 1367 Information Provisions, *available at* http://dhsconnect.dhs.gov/org/comp/mgmt/policies/Directives/002-02.pdf.

CISA will also provide with the Census Bureau a copy of the authorization letter submitted by each government organization requesting a .gov address. Authorization letters may contain letterheads that include information such as other officials' names phone numbers and addresses.

The Census Bureau will share with CISA:

- Name and title of the highest-elected or -ranking official
- Mailing address
- Email address
- Phone number

3(a) Does this Project, Program, or System collect, maintain, use, or disseminate Social Security numbers (SSN) or other types of stand-alone sensitive information?[5] If applicable, check all that apply.

☐ Social Security number ☐ Alien Number (A-Number) ☐ Tax Identification Number ☐ Visa Number ☐ Passport Number ☐ Bank Account, Credit Card, or other financial account number ☐ Driver's License/State ID Number	☐ Social Media Handle/ID ☐ Driver's License/State ID Number ☐ Biometric identifiers *(e.g., FIN, EID)* ☐ Biometrics.[6] *Please list modalities (e.g., fingerprints, DNA, iris scans): Click here to enter text.* ☐ Other. *Please list: Click here to enter text.*
3(b) Please provide the specific legal basis for the collection of SSN:	N/A

3(c) If the SSN is needed to carry out the functions and/or fulfill requirements of the Project, System, or Program, please explain why it is necessary and how it will be used.

N/A

3(d) If the Project, Program, or System requires the use of SSN, what actions are being taken to abide by Privacy Policy Instruction 047-01-010, *SSN Collection and Use Reduction*,[7] which requires the use of privacy-enhancing SSN alternatives when there are technological, legal, or regulatory limitations to eliminating the SSN? Note: *even if you are properly authorized to collect SSNs, you are required to use an alternate unique identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, privacy-enhancing alternatives should be taken, such as*

[5] Sensitive PII (or sensitive information) is PII that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. More information can be found in the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information, *available at* https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information.

[6] If related to IDENT/HART and applicable, please complete all Data Access Request Analysis (DARA) requirements. This form provides privacy analysis for DHS' IDENT, soon to be HART. The form replaces a PTA where IDENT is a service provider for component records. PRIV uses this form to better understand how data is currently shared, will be shared and how data protection within IDENT will be accomplished. IDENT is a biometrics service provider and any component or agency submitting data to IDENT is a data provider.

[7] *See* https://www.dhs.gov/publication/privacy-policy-instruction-047-01-010-ssn-collection-and-use-reduction.

masking, truncating, or encrypting the SSN, or blocking the display of SSNs in hard copy or digital formats.
N/A

4. How does the Project, Program, or System retrieve information?	☒ By a unique identifier.[8] Please list all unique identifiers used: All users have a unique username. ☐ By a non-unique identifier or other means. Please describe: *Click here to enter text.*

5. What is the records retention schedule(s) for the information collected for each category type (include the records schedule number)**?** *If no schedule has been approved, please provide proposed schedule or plans to determine it.* *Note: If no records schedule is in place or are unsure of the applicable records schedule, please reach out to the appropriate Records Management Office.*[9]	CISA is developing a records retention schedule for submission and approval by the National Archives Records Administration (NARA).
5(a) How does the Project, Program, or System ensure that records are disposed of or deleted in accordance with the retention schedule (e.g., technical/automatic purge, manual audit)**?**	All records will be retained as permanent until a records schedule establishing the appropriate disposition has been approved by NARA. CISA will work with NARA to develop an approved records retention schedules and policy for its systems. In addition, CISA information handling guidelines and operating procedures provide the procedures for the collection processing, retention, and dissemination of data.

6. Does this Project, Program, or System connect, receive, or share PII with any other DHS/Component projects, programs, or systems?[10]	☒ No. ☐ Yes. If yes, please list:

[8] 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.
[9] *See* http://dhsconnect.dhs.gov/org/comp/mgmt/ocio/IS2O/rm/Pages/RIM-Contacts.aspx
[10] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in IACS.

	Click here to enter text.
7. Does this Project, Program, or System connect, receive, or share PII with any external (non-DHS) government or non-government partners or systems?	☐ No. ☒ Yes. If yes, please list: • A contracted entity • U.S Census Bureau
8. Is this sharing pursuant to new or existing information sharing agreement (MOU, MOA, LOI, RTA, etc.)? *If applicable, please provide agreement as an attachment.*	New MOA establishing a joint statistical project between the U.S Census Bureau and CISA.
9. Does the Project, Program, or System or have a mechanism to track external disclosures of an individual's PII?	☐ No. What steps will be taken to develop and maintain the accounting: *Click here to enter text.* ☒ Yes. In what format is the accounting maintained: The program does not intend to allow unintentional external disclosure of an individual's PII. There are intended publications of security contact information (see question 7). In the event that PII is inadvertently disclosed, the program plans to work with the CISA Office of Chief Privacy Officer to appropriately mitigate issues surrounding the disclosure and follow the procedures required by the DHS Privacy Incident Handling Guidance.

10. Does this Project, Program, or System use or collect data involving or from any of the following technologies:	☐ Social Media ☐ Advanced analytics[11] ☐ Live PII data for testing ☒ No

11. Does this Project, Program, or System use data to conduct electronic searches,	☒ No.

[11] The autonomous or semi-autonomous examination of Personally Identifiable Information using sophisticated techniques and tools to draw conclusions. Advanced Analytics could include human-developed or machine-developed algorithms and encompasses, but is not limited to, the following: data mining, pattern and trend analysis, complex event processing, machine learning or deep learning, artificial intelligence, predictive analytics, big data analytics.

queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly indicative of terrorist or criminal activity on the part of any individual(s) (i.e., data mining)?[12] This does not include subject-based searches.	☐ Yes. If yes, please elaborate: *Click here to enter text.*
11(a) Is information used for research, statistical, or other similar purposes? If so, how will the information be de-identified, aggregated, or otherwise privacy-protected?	☒ No. ☐ Yes. If yes, please elaborate: *Click here to enter text.*

12. Does the planned effort include any interaction or intervention with human subjects[13] via pilot studies, exercises, focus groups, surveys, equipment or technology, observation of public behavior, review of data sets, etc. for research purposes	☒ No. ☐ Yes. If yes, please reach out to the DHS Compliance Assurance Program Office (CAPO) for independent review and approval of this effort.[14]

13. Does the Project, Program, or System provide role-based or additional privacy training for personnel who have access, in addition to annual privacy training required of all DHS personnel?	☐ No. ☒ Yes. If yes, please list: In addition to the annual privacy awareness training for CISA employees and contractors, system users and administrators also have requirements to complete: • Role-based Training for System Administrators.

[12] Is this a program involving pattern-based queries, searches, or other analyses of one or more electronic databases, where—
(A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals;
(B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and
(C) the purpose of the queries, searches, or other analyses is not solely—
(i) the detection of fraud, waste, or abuse in a Government agency or program; or
(ii) the security of a Government computer system.

[13] Human subject means a living individual about whom an investigator conducting research: (1) obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or (2) obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens.

[14] For more information about CAPO and their points of contact, please see: https://www.dhs.gov/publication/compliance-assurance-program-office or https://collaborate.st.dhs.gov/orgs/STCSSites/SitePages/Home.aspx?orgid=36. For more information about the protection of human subjects, please see DHS Directive 026-04: https://www.dhs.gov/sites/default/files/publications/mgmt/general-science-and-innovation/mgmt-dir_026-04-protection-of-human-subjects_revision-01.pdf.

	• Annual Role Based Cyber Privacy Training based on the Cybersecurity Information Handling Guidelines.

14. Is there a FIPS 199 determination?[15]	☒ No. ☐ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined Availability: ☐ Low ☐ Moderate ☐ High ☐ Undefined

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	**Beth LaGreca**
Date submitted to Component Privacy Office:	December 17, 2021
Concurrence from other Component Reviewers involved (if applicable):	Click here to enter text.
Date submitted to DHS Privacy Office:	December 20, 2021

Component Privacy Office Recommendation:
Please include recommendation below, including what new privacy compliance documentation is needed, as well as any specific privacy risks/mitigations, as necessary.

The CISA Office of the Chief Privacy Officer (OCPO) is conducting this PTA update to document the sharing of information between the Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Division (CSD) Capacity Building (CB) and the U.S. Census Bureau in connection with

[15] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

CISA's administration of the .gov Top-Level Domain (TLD) program. No operational changes have been made to the program since the previous PTA adjudication. The program name provided on this PTA has been changed from ".gov TLD registry and registrar" to ".gov Top Level Domain (TLD) Program".

OCPO recommends that the .gov TLD Program is privacy sensitive, requiring PIA and SORN coverage. We also recommend that a Privacy Act Statement be placed on the .gov registration page.

PIA coverage is provided by DHS General Contact Lists PIA, DHS/ALL/PIA-006 Department of Homeland Security General Contact Lists, published June 15, 2007. SORN coverage is provided by DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, published November 25, 2008 and DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), published November 27, 2012.

Privacy Act Statement to be placed on the .gov registration page –

Privacy Act Statement

Authority: The DOTGOV Act of 2020 (6 U.S.C. § 665) authorizes the Cybersecurity and Infrastructure Security Agency (CISA) to make .gov domains and supporting services available to eligible entities.

Purpose: CISA will use this information to ensure that .gov domains are registered and maintained only by authorized authorities. CISA and the U.S. Census Bureau will exchange data related to U.S.-based government organizations.

Routine Uses: The information requested will be shared as a routine use to the Census Bureau as part of the agreement between the Census Bureau and CISA. A complete list of routine uses can be found in the DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System of Records (November 25, 2008, 73 FR 71659). The Department's full list of system of records notices can be found on the Department's website at https://www.dhs.gov/system-records-notices-sorns.

Disclosure: Providing this information is voluntary. However, failure to provide this information will prevent CISA from fulfilling your request for a .gov domain and supporting services.

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	**Kattina Do**
DHS Privacy Office Approver (if applicable):	**Riley Dean**
Workflow Number:	0021620
Date approved by DHS Privacy Office:	December 21, 2021
PTA Expiration Date	December 21, 2024

DESIGNATION

Privacy Sensitive System:	Yes
Category of System:	Program If "other" is selected, please describe: *Click here to enter text.*
Determination:	☒ Project, Program, System in compliance with full coverage ☐ Project, Program, System in compliance with interim coverage ☐ Project, Program, System in compliance until changes implemented ☐ Project, Program, System not in compliance
PIA:	**System covered by existing PIA** • DHS/ALL/PIA-006 General Contact Lists
SORN:	**System covered by existing SORN** • 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

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above, and any further action(s) that must be taken by Component.

CISA is submitting this updated PTA to discuss the .gov Top-Level Domain (TLD) Program. This update is to include, the information sharing between the CISA Cybersecurity Division (CSD) Capacity Building (CB) and the U.S. Census Bureau in connection with CISA's administration of the .gov Top-Level Domain (TLD) program, and the program name .gov TLD registry and registrar is now .gov Top Level Domain (TLD) Program, and no operational changes have been made to the program since the previous PTA adjudication.

The Domain Name System (DNS) is the internet service that translates between the names humans prefer and the numbers computers need to navigate to a website or send an email address. The .gov registry is

the DNS infrastructure that makes the TLD and all registered .gov domain names available over the internet. The DOTGOV Online Trust in Government Act of 2020 transferred responsibility for the .gov TLD from the GSA to CISA.

The information collected:

- .gov Registration - U.S.-based government organizations requesting a .gov domain address must provide contact information including first name, last name, governmental organization phone number, email address, and mailing address.
- Census Bureau and CISA Information Sharing Project - specific information about individuals CISA will disseminate to the Census Bureau: name of the authorizing authority, administrative contact, technical contact and security contact, physical addresses, and email addresses. CISA will also provide with the Census Bureau a copy of the authorization letter submitted by each government organization requesting a .gov address. Authorization letters may contain letterheads that include information such as other officials' names phone numbers and addresses.
- Census Bureau will share with CISA: name and title of the highest-elected or -ranking official, mailing address, email address, and phone number

The DHS Privacy Office (PRIV) finds that this program 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-006 DHS General Contact Lists, which covers the collection of contact information to conduct agency operations.

PRIV finds that a SORN is required because information is retrieved by a unique identifier. PRIV agrees with CISA Privacy and finds that SORN coverage is provided by DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, which covers the collection of PII to provision access to DHS IT. In addition, SORN coverage is provided by DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), which covers the Department of Homeland Security to collect a discreet set of personally identifiable information in order to provide authorized individuals access to, or interact with DHS information technology resources, and allow DHS to track use of DHS IT resources.

CISA is required to use the Privacy Act Statement attached to this PTA.