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 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 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)

SUMMARY INFORMATION

Project, Program, or System Name:	**National Initiative for Cybersecurity Careers and Studies (NICCS) Training Catalog Batch Data**		
Component or Office:	Cybersecurity and Infrastructure Security Agency (CISA)	**Office or Program:**	Office of the Chief Learning Officer (OCLO)
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 4, 2012	**Pilot launch date:**	December 21, 2012
Date of last PTA update	N/A	**Pilot end date:**	March 14, 2016
ATO Status (if applicable):[1]	Choose an item.	**Expected ATO/ATP/OA date (if applicable):**	Click here to enter a date.

PROJECT, PROGRAM, OR SYSTEM MANAGER

Name:	**Shannon Nguyen**		
Office:	OCLO	**Title:**	Program Manager
Phone:	202-657-3298	**Email:**	shannon.nguyen@hq.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	**Feda Handac**		
Phone:	678-428-9203	**Email:**	feda.handac@associates.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.

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: New PTA
This new PTA is being conducted for the Cybersecurity and Infrastructure Security Agency (CISA) Office of the Chief Learning Officer (OCLO) National Initiative for Cybersecurity Careers and Studies (NICCS) Training Catalog Batch Data. This form allows organization and academic institutions to provide course-specific technical information to NICCS regarding how their training courses map to the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework) Specialty Areas. This PTA replaces the legacy NICCS PTA[2], which is no longer valid as the information previously covered by the legacy PTA is now covered by PTAs respective to the individual collections of information, and not just one programmatic PTA. NICCS is a public-facing website, available at niccs.cisa.gov, created to provide the general public with the resources necessary to expand their knowledge of cybersecurity through training and education courses. . The courses are listed in the NICCS Education and Training Catalog, available at niccs.cisa.gov/education-training/catalog, serves asa central location for cybersecurity professionals to find cybersecurity-related courses online and in person.. Organizations or academic institutions interested in listing courses with NICCS must first complete a vendor vetting process[3] in order to be considered for inclusion in the NICCS Education and Training Catalog. Once approved, organizations and academic institutions are asked to provide technical information ("training catalog batch data") to NICCS regarding how their training courses map to the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework) Specialty Areas. Course mapping to these Specialty Areas allows users to tailor their individual coursework and is dependent upon the training catalog batch data to do so. The training catalog batch data is technical in nature, is not privacy sensitive, and does not include personally identifiable information. The training catalog batch data is submitted to the CISA NICCS Supervisory Office (SO) for review. Once approved, the organization/academic institution's course is listed in the NICCS Education and Training Catalog.

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[4] ☐ Members of the public ☐ U.S. Persons (U.S citizens or lawful permanent residents)

[2] *See* PTA, CISA – NICCS, 20190722, PRIV Final.pdf
[3] *See* PTA, CISA – Vendor Vetting Form
[4] 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.

	☐ Non-U.S. Persons ☐ DHS Employees/Contractors (list Components): *Click here to enter text.* ☐ Other federal employees or contractors (list agencies): *Click here to enter text.*
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)[5] ☐ Refugees/Asylees ☐ Other. Please list: *Click here to enter text.*

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

Specific information about individuals is not collected, maintained, used or disseminated. Training Providers are asked to provide technical information regarding how their training courses map to the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework) Specialty Areas. Below is the information provided and a brief description of each.

COURSE-SPECIFIC TECHNICAL INFORMATION PROVIDED TO NICCS		
Column Name	**Required**	**Description**
tccid	NO	The NICCS-provided course id of the record.
name	YES	The title of the training course.
provider	YES	The name of the organization, as it will display on the NICCS website.
tcccatnbr	NO	The Catalog Number of the training course.
tcclocalnbr	NO	The Provider-specified Course ID
tcccae	NO	Identifying providers who have been recognized as NCAE-C Designated Institution.
tcccourl	YES	The course URL of the training course.
description	YES	Training course description
tccprereq	YES	Training course prerequisites

[5] 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.

tccproflvl	YES	Training course overall proficiency level
tcctrainpur	YES	Training course training purposes
tccaudience	YES	Training course audiences
tccobjective	YES	Training course objectives
tccdelmethod	YES	The course delivery method of the training course.
tccspecarea	YES	The specialty area of the training course
tcccourseloc	NO	A JSON-formatted list of addresses where the training course is offered.
softdelete	NO	A field to indicate the course should be unpublished from the NICCS training catalog.
tcccomp	YES	The competency area of the training course
tccworkrole	YES	The work role of the training course

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?[6] 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
☐ Biometric identifiers *(e.g., FIN, EID)*
☐ Biometrics.[7] *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

[6] 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.

[7] 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.

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*,[8] 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 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.[9] Please list all unique identifiers used: *Click here to enter text.* ☒ By a non-unique identifier or other means. Please describe: Information is retrieved using the catalog number of the training course.
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.*[10]	General Records Schedule 3.1- Item 051 General Technology Management Records: Data Administration Records.
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)**?**	CISA has worked with the National Archives and Records Administration (NARA) to identify an approved records retention schedules and policy for its systems. Records will be purged from the DHS database after five years, per DHS existing policy. CISA cybersecurity analysts are also required to review all data collected and determine if it is necessary to analyze or understand the cybersecurity

[8] *See* https://www.dhs.gov/publication/privacy-policy-instruction-047-01-010-ssn-collection-and-use-reduction.
[9] 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.
[10] *See* http://dhsconnect.dhs.gov/org/comp/mgmt/ocio/IS2O/rm/Pages/RIM-Contacts.aspx

	threat. 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?[11]	☒ No. ☐ Yes. If yes, please list:
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:
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.*	Choose an item. Please describe applicable information sharing governance in place: N/A
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: N/A ☐ Yes. In what format is the accounting maintained:
10. Does this Project, Program, or System use or collect data involving or from any of the following technologies:	☐ Social Media ☐ Advanced analytics[12] ☐ Live PII data for testing ☒ No
11. Does this Project, Program, or System use data to conduct electronic searches, 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)	☒ No. ☐ Yes. If yes, please elaborate:

[11] 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.
[12] 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.

(i.e., data mining)?[13] This does not include subject-based searches.	
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:
12. Does the planned effort include any interaction or intervention with human subjects[14] 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.[15]
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:
14. Is there a FIPS 199 determination?[16]	☒ No. ☐ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined

[13] 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.

[14] 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.

[15] 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.

[16] 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.

	Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined Availability: ☐ Low ☐ Moderate ☐ High ☒ Undefined

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	**Donna Hellberg**
Date submitted to Component Privacy Office:	**November 14, 2022**
Concurrence from other Component Reviewers involved (if applicable):	*Click here to enter text.*
Date submitted to DHS Privacy Office:	**November 15, 2022**

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 NICCS program provides an invaluable resource to the cybersecurity industry by making courses and their training providers available to the public. Once vetted and approved, NICCS program staff ask training providers to complete a technical mapping of their course to its applicable NICE Framework Specialty Areas. This process allows users to narrow search results for training courses down to their desired areas of cybersecurity education and training.

The information collected via NICCS Training Catalog Batch Data is not privacy sensitive and does not include personally identifiable information.

Separate privacy compliance documentation used in conjunction with the NICCS Training Catalog Batch Data in which privacy sensitive information is collected. Information submitted on that form is not maintained on the website but rather in the program's document repository restricted to program personnel only. Please see the NICCS Vendor Vetting Forms PTA for more information.

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	**Kattina Do**
DHS Privacy Office Approver (if applicable):	**Schuntel Reddock**
Workflow Number:	**0023424**
Date approved by DHS Privacy Office:	November 17, 2022
PTA Expiration Date	November 17, 2025

DESIGNATION

Privacy Sensitive System:	No
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:	Choose an item. *Click here to enter text.*
SORN:	Choose an item. *Click here to enter text.*

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 PTA to discuss the National Initiative for Cybersecurity Careers and Studies (NICCS) Training Catalog Batch Data. NICCS is a public-facing website, available at niccs.cisa.gov, created to provide the general public with the resources necessary to expand their knowledge of cybersecurity through training and education courses. Organizations or academic institutions interested in listing courses with NICCS must first complete a vendor vetting process in order to be considered for inclusion in the NICCS Education and Training Catalog. The training catalog batch data is technical in nature, is not privacy sensitive, and does not include personally identifiable information. The training catalog batch data is submitted to the CISA NICCS Supervisory Office (SO) for review. Once approved, the organization/academic institution's course is listed in the NICCS Education and Training Catalog.

Specific information about individuals is not collected, maintained, used or disseminated. Training Providers are asked to provide technical information regarding how their training courses map to the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework) Specialty Areas.

The DHS Privacy Office (PRIV) finds that this program is not privacy-sensitive because PII is not collected, and therefore a PTA is sufficient at this time.