Supporting Statement for Paperwork Reduction Act Submissions

Title: "Cybersecurity Education & Awareness Office (CE&A) National Initiative for Cybersecurity Careers and Studies (NICCS) Cybersecurity Training and Education Catalog (Training/Workforce Development Catalog) Collection

OMB Control Number: 1670-0030

Collection Instruments:

1. NICCS Cybersecurity Training Course Web Form
2. NICCS Vendor Vetting Web Form
3. NICCS Certification Course Form
4. NICCS Mapping Tool

A. Justification

1. Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection. Attach a copy of the appropriate section of each statute and regulation mandating or authorizing the collection of information.

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 seeks to collect information from organizations and academic institutions regarding their course specific technical information to NICCS regarding how their training courses map to the National Initiative for Cybersecurity (NICE) Workforce Framework for Cybersecurity (NICE Framework) Specialty Areas.

The NICCS website is a national online resource for cybersecurity awareness, education, talent management, and professional development and training. Its mission is to provide comprehensive cybersecurity resources to the public.

To promote cybersecurity education, and to provide a comprehensive resource for the Nation, NICCS developed the Cybersecurity Training and Education Catalog. The NICCS Education and Training Catalog is a central location to help cybersecurity professionals of all skill levels find cybersecurity-related courses online and in person across the nation. All of the courses are aligned to the specialty areas of The Workforce Framework for Cybersecurity (NICE Framework). Organizations and or academic institution interested in listing courses with NICCS are requested to complete a vendor vetting process 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. Then upon further review and approval, the organization/academic institution's course is listed in the NICCS Education and Training Catalog.

The cyber-specific authorities to receive such information support the Department's general authority to receive information from any federal or non-federal entity in support of the mission responsibilities of the Department. Section 201 of the Homeland Security Act authorizes the Secretary "[t]o access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information, in support of the mission responsibilities of the Department." 6 U.S.C. § 121(d)(1); see also 6 U.S.C. § 121(d)(12). The following authorities also permit DHS to collect this information: Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. 3546; Presidential Policy Directive (PPD)-21, Critical Infrastructure Identification, Prioritization, and Protection (2003); and National Security Presidential Directive (NSPD)-54/HSPD-23, Cybersecurity Policy (2009).

Note: Any information received from the public in support of the NICCS Cybersecurity Training and Education Catalog is completely voluntary. Organizations and individuals who do not provide information can still utilize the NICCS website and Catalog without restriction or penalty. An organization or individual who wants their information removed from the NICCS website and/or Cybersecurity Training and Education Catalog can e-mail the NICCS Supervisory Office. There are no requirements for a provider to fill out a specific form for their information to be removed; standard email requests will be honored.

2. Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection.

CISA OCLO seeks to utilize four separate forms in to order to collect the requested information from organizations and academic institutions. CISA OCLO will use the NICCS Cybersecurity Training Course Form and the NICCS Cybersecurity Certification Form to collect information via the publicly accessible website called the National Initiative for Cybersecurity Careers and Studies (NICCS) website (https://niccs.cisa.gov). Collected information from these two forms include the following requested information categories below and will be included in the Cybersecurity Training and Education Catalog that is hosted on the NICCS website.

Types of information collected by the NICCS Cybersecurity Training Course Form:
Training/WFD Provider Name and Address
Training/WFD Provider Point of Contact information (name, e-mail, phone number)
Training/WFD Provider Logo
Training Name
Training Description
Training Catalog Number
Training URL
Training Purpose

National Cybersecurity Workforce Framework Specialty Area
National Cybersecurity Workforce Framework Role
Intended Audience
Learning Objective(s)
Training Proficiency Level
Prerequisite(s)
Delivery

Types of information collected by the NICCS Cybersecurity Certification Form:
Certification Provider Name and Address
Certification Provider Point of Contact information (name, e-mail, phone number)
Certification Provider Logo
Certification Name
Certification Description
Certification Catalog Number
Certification URL
Certification Purpose
National Cybersecurity Framework Specialty Area
National Cybersecurity Workforce Framework Role
Intended Audience
Learning Objective(s)
Certification Proficiency Level
Prerequisite(s)
Delivery

The NICCS Supervisory Office within OCLO will use information collected from the NICCS Vendor Vetting Form to primarily manage communications with the training/workforce development providers; this collected information will not be shared with the public and is intended for internal use only. The following information categories to be collected on the NICCS Vendor Vetting form is below. Additionally, this information will be used to validate training providers before uploading their training and certification information to the Training Catalog.

Type of information collected by the NICCS Vendor Vetting Form:
Organization Name and Address
Organization Point of Contact information (name, e-mail, phone number, etc.)
Organization URL
Training Provider listed on the General Services Administration schedule?
Is the Training Provider credentialed from National Centers of Academic Excellence?
Is the Training Provider an approved federal agency or department training provider?
Has the Training Provider been in business for at least a year?
How often does the Training Provider deliver/conduct cybersecurity training?
Proof of business entity license.
Training Course standards.
Training Provider Point of Contact Electronic Signature.

The NICCS Supervisory Office will use information collected from the NICCS Mapping Tool Form to provide an end user with information of how their position or job title aligns to the new Cybersecurity Framework 1.1. This collection of inputs and output (in the form of a report) will be savable by the end user on their computer to be uploaded at a later time for further use if required. The following information categories to be collected on the NICCS Mapping Tool form

is below. This collected information will not be shared with the public and is intended for internal use only.

Types of information collected by the NICCS Mapping Tool Form:
Select the statement below that best describes this position's work at a high level
Select the statement which specifically describes the position's work (Specialty Area)
Add Filter option: Intelligence, Occupational, Series Number
Select the statements below that most specifically describe the position's work (Task)
Select all knowledge, skills, or abilities possessed by this position (KSA)
Status Position
Position Description (optional)
Organization Title
Series
OPM Job Announcement Number
Government Department or Agency
Division / Section / Component:
Location

3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses, and the basis for the decision for adopting this means of collection. Also describe any consideration of using information technology to reduce burden.

The information will be collected via fully electronic web forms or partially electronic via email. Collection will be coordinated between the public and NICCS via e-mail (niccs@hq.dhs.gov).

The following forms are fully electronic:

- NICCS Vendor Vetting Web Form
- NICCS Cybersecurity Training Course Web Form
- NICCS Mapping Tool Web Form

The following forms are partially electronic:

- NICCS Certification Course Form

All information collected from the NICCS Cybersecurity Training Course Web Form, and the NICCS Certification Course Form will be stored in the public accessible NICCS Cybersecurity Training and Education Catalog (https://niccs.cisa.gov/education-training/catalog).

The NICCS Supervisory Office will electronically store information collected via the NICCS Vendor Vetting Form. This information collected will not be publicly accessible.

Information collected for the NICCS Certification Course Form is collected via email in a CSV format, and then compiled by the NICCS staff for upload to the NICCS Education and Training Catalog.

Information collected by the NICCS Mapping Tool is not being stored by NICCS. The information collected will not be publicly accessible. Users have the option of saving their input and results to be used at a later time, and the information would only be stored the user's device.

CISA conducted additional usability testing on all the forms to help with verification of the burden hours and to verify the ease of use. The usability testing participants confirmed the accuracy of the burden hours and had no difficult traversing through the documents. Based on the feedback received, CISA made minor changes to the forms for clarification and grammar. The burden hours were updated and modified due to historical numbers received and respondent feedback.

4. Describe efforts to identify duplication. Show specifically why any similar information already available cannot be used or modified for use for the purposes described in Item 2 above.

After review of www.reginfo.gov, this information is not collected in any form, and therefore is not duplicated elsewhere.

5. If the collection of information impacts small businesses or other small entities (Item 5 of OMB Form 83-I), describe any methods used to minimize.

Impact to small businesses or other small entities is determined to be insignificant based on the fact that all information is completely voluntary and requires insignificant amount of time to provide (via e-mail).

6. Describe the consequence to Federal/DHS program or policy activities if the collection of information is not conducted, or is conducted less frequently, as well as any technical or legal obstacles to reducing burden.

The Cybersecurity Training/Workforce Development and Education Catalog exists solely to share cybersecurity training, workforce development and education information with the general public, specifically for cybersecurity professionals. NICCS has identified the type of information and collection frequency in order to provide relevant, accurate, and timely information.

7. Explain any special circumstances that would cause an information collection to be conducted in a manner:

(a) Requiring respondents to report information to the agency more often than quarterly.

(b) Requiring respondents to prepare a written response to a collection of information in fewer than 30 days after receipt of it.

(c) Requiring respondents to submit more than an original and two copies of any document.

(d) Requiring respondents to retain records, other than health, medical, government contract, grant-in-aid, or tax records for more than three years.

(e) In connection with a statistical survey, that is not designed to produce valid and reliable results that can be generalized to the universe of study.

(f) Requiring the use of a statistical data classification that has not been reviewed and approved by OMB.

(g) That includes a pledge of confidentiality that is not supported by authority established in statute or regulation, that is not supported by disclosure and data security policies that are consistent with the pledge, or which unnecessarily impedes sharing of data with other agencies for compatible confidential use.

(h) Requiring respondents to submit proprietary trade secret, or other confidential information unless the agency can demonstrate that it has instituted procedures to protect the information's confidentiality to the extent permitted by law.

The special circumstances contained in item 7 of the Supporting Statement are not applicable to this information collection.

8. Federal Register Notice:

a. Provide a copy and identify the date and page number of publication in the Federal Register of the agency's notice soliciting comments on the information collection prior to submission to OMB. Summarize public comments received in response to that notice and describe actions taken by the agency in response to these comments. Specifically address comments received on cost and hour burden.

b. Describe efforts to consult with persons outside the agency to obtain their views on the availability of data, frequency of collection, the clarity of instructions and recordkeeping, disclosure, or reporting format (if any), and on the data elements to be recorded, disclosed, or reported.

c. Describe consultations with representatives of those from whom information is to be obtained or those who must compile records. Consultation should occur at least once every three years, even if the collection of information activities is the same as in prior periods. There may be circumstances that may preclude consultation in a specific situation. These circumstances should be explained.

	Date of Publication	**Volume #**	**Number #**	**Page #**	**Comments Addressed**
60Day Federal Register Notice:	6/20/2024	89	119	51892-51894	0
30-Day Federal	9/5/2025	90	170	42977-	0

Register Notice				42978	

A 60-day notice for comments was published in the Federal Register on 6/20/2024. No comments were received related to the 60-day notice.

A 30-day notice for comments was published in the Federal Register on 9/5/2025. 0 comments were received related to the 30-day notice.

9. Explain any decision to provide any payment or gift to respondents, other than remuneration of contractors or grantees.

There is no offer of monetary or material value for this information collection.

10. Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation, or agency policy.

There is no assurance of confidentiality provided to the respondents. This collection is a non-privacy sensitive collection; therefore, does not require a Privacy Impact Assessment (PIA) or Systems of Records Notice (SORN).

11. Provide additional justification for any questions of a sensitive nature, such as sexual behavior and attitudes, religious beliefs, and other matters that are commonly considered private. This justification should include the reasons why the agency considers the questions necessary, the specific uses to be made of the information, the explanation to be given to persons from whom the information is requested, and any steps to be taken to obtain their consent.

There are no questions of sensitive nature.

12. Provide estimates of the hour burden of the collection of information. The statement should:

a. Indicate the number of respondents, frequency of response, annual hour burden, and an explanation of how the burden was estimated. Unless directed to do so, agencies should not conduct special surveys to obtain information on which to base hour burden estimates. Consultation with a sample (fewer than 10) of potential respondents is desired. If the hour burden on respondents is expected to vary widely because of differences in activity, size, or complexity, show the range of estimated hour burden, and explain the reasons for the variance. Generally, estimates should not include burden hours for customary and usual business practices.

To estimate the burden associated with this collection, NICCS estimates the number of respondents, the number of responses per respondent and the time burden per response for each of the four instruments accounted for in this collection. Table X presents the number of respondents, responses, and time burdens, in hours, for each of the instruments.

Table X: Annual Time Burden

Type of Respondent	Form Name	No. Of Respondents	No. Of Responses per Respondent	Total Annual No. Of Responses	Avg. Burden per Response (in hours)	Total Annual Burden (in hours)
Academic Institutions; Federal Government Organizations, Agencies, and Departments; Private Cybersecurity Training Providers	NICCS Cybersecurity Training Course Web Form	50	1	50	0.25 (15 minutes)	12.5
Academic Institutions; Federal Government Organizations, Agencies, and Departments; Private Cybersecurity Training Providers	NICCS Certification Course Form	100	1	100	2	200
Academic Institutions; Federal Government Organizations, Agencies, and Departments; Private Cybersecurity Training Providers	NICCS Vendor Vetting Criteria Web Form	50	1	50	2	100
Federal Government, Private Sector, Industry, Academia, Local Government, Individual	NICCS Mapping Tool	300	1	300	0.25 (15 Minutes)	75
Total		**500**		**500**	0.775	**387.5**

Note: Totals may not sum due to rounding

To estimate the cost associated with the burden for these instruments, NPPD calculated an average wage for all respondents, based on the mean hourly wages for 1 occupation within the education sector. Table Y presents the occupations and their wages.

Table Y: Occupations Used to Estimate Average Wage

	Information Security Analysts	Web Developer	Computer Network Architects	Network and Computer Systems Administrators
Educational Services, Privately Owned[1]	$49.70	$36.03	$55.36	$40.78
Technical and Trade Schools, Privately Owned[2]	$46.54	$32.53	$62.53	$33.69
Technical and trade Schools, Local Government Owned[3]	$46.54	$32.53	$62.53	$38.05
Technical and Trade Schools, State Government Owned[4]				$38.05
Colleges, Universities, and Professional Schools, Privately Owned[5]	$50.22	$38.48	$53.72	$41.50

Note: Totals may not sum due to rounding

Taking the average of these 17 mean wages results in an average hourly wage of $44.63. NPPD then applies a load factor of 1.4155[6] to this average wage to obtain a fully loaded average hourly wage of $63.18. The total annual burden for this collection is $24,482. Table Z presents the monetized burden of this collection, by instrument.

[1] https://www.bls.gov/oes/2022/may/611000_5.htm#15-0000
[2] https://www.bls.gov/oes/2022/may/611500_5.htm#15-0000
[3] https://www.bls.gov/oes/2022/may/611500_3.htm#15-0000
[4] https://www.bls.gov/oes/2022/may/611500_2.htm#15-0000
[5] https://www.bls.gov/oes/2022/may/611300_5.htm#15-0000
[6] Load factor based on BLS Employer Cost for Employee Compensation, as of December 12, 2023. Load factor = Employer cost for employee compensation ($41.53) / wages and salaries ($29.34) = 1.415474 Employer Costs for Employee Compensation News Release - 2023 Q03 Results (bls.gov)

Table Z: Annual Monetized Burden

Type of Respondent	Form Name	Total Annual Burden (in hours)	Loaded Hourly Wage	Annual Burden
Academic Institutions; Federal Government Organizations, Agencies, and Departments; Private Cybersecurity Training Providers	NICCS Cybersecurity Training Course Web Form	12.5	$63.18	$789.73
Academic Institutions; Federal Government Organizations, Agencies, and Departments; Private Cybersecurity Training Providers	NICCS Certification Course Form	200	$63.18	$12,636
Academic Institutions; Federal Government Organizations, Agencies, and Departments; Private Cybersecurity Training Providers	NICCS Vendor Vetting Criteria Web Form	100	$63.18	$6,318
Federal Government, Private Sector, Industry, Academia, Local Government, Individual	NICCS Mapping Tool	75	$63.18	$4,738
Total		**387.5**		**$24,482**

Note: Totals may not sum due to rounding

13. Provide an estimate of the total annual cost burden to respondents or record keepers resulting from the collection of information. (Do not include the cost of any hour burden shown in Items 12 and 14.)

There are no record keeping, capital, start-up or maintenance costs associated with this information collection.

14. Provide estimates of annualized cost to the Federal Government. Also, provide a description of the method used to estimate cost, which should include quantification of hours, operational expenses (such as equipment, overhead, printing and support staff), and any other expense that would have been incurred without this collection of information. You may also aggregate cost estimates for Items 12, 13, and 14 in a single table. @

The estimated annualized cost to the Federal government for this collection is calculated to be approximately $161,490. The following method was used to estimate the cost (based on FY17 General Schedule Grade 9, step 5, WASHINGTON-BALTIMORE-NORTHERN VIRGINIA, DC-MD-VA-WV-PA locality, fully loaded annual pay of $131,165 ($77,525 x 1.6919 benefit multiplier[7] = $131,165)):

- Cost of NICSS SO to review NICCS Vetting Criteria Form: 1 personnel x 10% annual time = $13,117
- Cost of NICCS SO to review NICCS Training Course Web Form: 1 personnel x 5% annual time = $6,558
- Cost of NICCS SO to review NICCS Certification Course Form: 1 personnel x 20% annual time = $26,233
- Cost of Training Catalog DBA: 25% annual time= ~$32,791
- Cost of Training Catalog web developers: 1 personnel x 25% annual time = $32,791
- Cost of server to host Training Catalog (recurring annually): = $50,000

Total: $161,490

15. Explain the reasons for any program changes or adjustments reported in Items 13 or 14 of the OMB Form 83-I. Changes in hour burden, i.e., program changes or adjustments made to annual reporting and recordkeeping **hour** and **cost** burden. A program change is the result of deliberate Federal government action. All new collections and any subsequent revisions of existing collections (e.g., the addition or deletion of questions) are recorded as program changes. An adjustment is a change that is not the result of a deliberate Federal government action. These changes that result from new estimates or actions not controllable by the Federal government are recorded as adjustments.

The updates to the collection include: The total burden hours and costs was reduced since the Training Catalog and other tool included are in maintenance mode and is updated as needed. The level of effort to support this is not as great as it was when it was first developed.
There were no changes to the content of the information collections and no changes to the information being collected.

16. For collections of information whose results will be published, outline plans for tabulation and publication. Address any complex analytical techniques that will be used. Provide the time schedule for the entire project, including beginning and ending dates of the collection of information, completion of report, publication dates, and other actions.

[7] CBO. Comparing the Compensation of Federal and Private-Sector Employees, 2011 to 2015. April 2017. https://www.cbo.gov/publication/52637
According to Table 4, Average Total Compensation for all levels of education is $64.80. According to Table 2, Average wages for all levels of education is $38.30. We estimate the compensation factor by dividing total compensation by average wages.

All information collected from NICCS Cybersecurity Training Course Web Form, and the NICCS Certification Course Form will be stored in the publicly accessible NICCS Cybersecurity Training/Workforce Development and Education Catalog (NICCS Education & Training Catalog | NICCS (cisa.gov).

No complex analytical techniques will be used.

Information will be published to the NICCS Cybersecurity Training/Workforce Development and Education Catalog on a regular, ongoing basis, after each course has been reviewed, vetted, and approved for publishing. This change was added based on input received from the public.

This project has no set end date.

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain reasons that display would be inappropriate.

NICCS will display the expiration date for OMB approval of this information collection.

18. Explain each exception to the certification statement identified in Item 19 "Certification for Paperwork Reduction Act Submissions," of OMB Form 83-I.

NICCS does not request an exception to the certification of this information collection.