

## Supporting Statement for Paperwork Reduction Act Submissions

**Title: Department of Homeland Security (DHS) 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 cyber-specific authorities to receive 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).

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

To promote cybersecurity education, and to provide a comprehensive resource for the Nation, NICE developed the Cybersecurity Training and Education Catalog. The Cybersecurity Training and Education Catalog will be hosted on the NICCS Portal. Training Course and certification information will be included in the Training/Workforce Development Catalog.

Note: Any information received from the public in support of the NICCS Portal and Cybersecurity Training and Education Catalog is completely voluntary. Organizations and individuals who do not provide information can still utilize the NICCS Portal and Cybersecurity Training and Education Catalog without restriction or penalty. An organization or individual who wants their information removed from the NICCS Portal 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.

Department of Homeland Security (DHS) Cybersecurity Education & Awareness Office (CE&A) uses the collected information from the NICCS Cybersecurity Training Course Form and the NICCS Cybersecurity Certification Form and displays it on a publicly accessible website called the National Initiative for Cybersecurity Careers and Studies (NICCS) Portal (<http://niccs.us-cert.gov/>). Collected information from these two forms will be included in the Cybersecurity Training and Education Catalog that is hosted on the NICCS Portal.

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

<b>Types of information collected by the NICCS Cybersecurity Certification Form:</b>
<b>Certification Provider Name and Address</b>
<b>Certification Provider Point of Contact information (name, e-mail, phone number)</b>
<b>Certification Provider Logo</b>
<b>Certification Name</b>
<b>Certification Description</b>
<b>Certification Catalog Number</b>
<b>Certification URL</b>
<b>Certification Purpose</b>
<b>National Cybersecurity Framework Specialty Area</b>
<b>National Cybersecurity Workforce Framework Role</b>
<b>Intended Audience</b>

**Learning Objective(s)**

**Certification Proficiency Level**

**Prerequisite(s)**

**Delivery**

The DHS CE&A NICCS Supervisory Office 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. 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 DHS CE&A 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. 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 DHS CE&A 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 (<http://niccs.us-cert.gov/training/training-home>).

The NICCS Supervisory Office will electronically store information collected via the NICCS Vetting Criteria 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 Portal.

Information collected by the NICCS Mapping Tool is not being stored by DHS CE&A. 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.

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](http://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. DHS CE&A 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.

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

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

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

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

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

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

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

(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.

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

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

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

- (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.

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

- (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.

	<b>Date of Publication</b>	<b>Volume #</b>	<b>Number #</b>	<b>Page #</b>	<b>Comments Addressed</b>
<i>60Day Federal Register Notice:</i>	Monday, November 20, 2017	82	222	55110	0
<i>30-Day Federal Register Notice</i>	Tuesday, February, 27, 2018	83	39	8496	0

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, NPPD 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 Form	350	3	1,050	0.5	525
Academic Institutions; Federal Government Organizations, Agencies, and Departments; Private Cybersecurity Training Providers	NICCS Certification Course Form	300	3	900	1	900
Academic Institutions; Federal Government Organizations, Agencies, and Departments; Private Cybersecurity Training Providers	NICCS Vetting Criteria Web Form	350	1	350	0.5	175
Federal Government, Private Sector, Industry, Academia, Local Government, Individual	NICCS Mapping Tool	350	1	350	0.25	88
<b>Total</b>		<b>1,350</b>		<b>2,650</b>		<b>1,688</b>

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 eleven occupations 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 <sup>1</sup>	\$39.54	\$33.00	\$35.57	
Technical and Trade Schools, Privately Owned <sup>2</sup>	\$44.69	\$31.82	\$40.43	
Technical and trade Schools, Local Government Owned <sup>3</sup>				\$31.32
Technical and Trade Schools, State Government Owned <sup>4</sup>				\$27.80
Colleges, Universities, and Professional Schools, Privately Owned <sup>5</sup>	\$43.85	\$32.38	\$34.79	

Note: Totals may not sum due to rounding

Taking the average of these eleven mean wages results in an average hourly wage of \$35.93. NPPD then applies a load factor of 1.4639<sup>6</sup> to this average wage to obtain a fully loaded average hourly wage of \$52.59. The total annual burden for this collection is \$88,775. Table Z presents the monetized burden of this collection, by instrument.

**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 Form	525	\$52.59	\$27,610

<sup>1</sup> [https://www.bls.gov/oes/2016/may/611000\\_5.htm#15-0000](https://www.bls.gov/oes/2016/may/611000_5.htm#15-0000)

<sup>2</sup> [https://www.bls.gov/oes/2016/may/611500\\_5.htm#15-0000](https://www.bls.gov/oes/2016/may/611500_5.htm#15-0000)

<sup>3</sup> [https://www.bls.gov/oes/2016/may/611500\\_3.htm#15-0000](https://www.bls.gov/oes/2016/may/611500_3.htm#15-0000)

<sup>4</sup> [https://www.bls.gov/oes/2016/may/611500\\_2.htm#15-0000](https://www.bls.gov/oes/2016/may/611500_2.htm#15-0000)

<sup>5</sup> [https://www.bls.gov/oes/2016/may/611300\\_5.htm#15-0000](https://www.bls.gov/oes/2016/may/611300_5.htm#15-0000)

<sup>6</sup> Load factor based on BLS Employer Cost for Employee Compensation, as of June 9, 2017. Load factor = Employer cost for employee compensation (\$35.28) / wages and salaries (\$24.10) = 1.4639 <https://www.bls.gov/news.release/ecec.nr0.htm>

Academic Institutions; Federal Government Organizations, Agencies, and Departments; Private Cybersecurity Training Providers	NICCS Certification Course Form	900	\$52.59	\$47,333
Academic Institutions; Federal Government Organizations, Agencies, and Departments; Private Cybersecurity Training Providers	NICCS Vetting Criteria Web Form	175	\$52.59	\$9,204
Federal Government, Private Sector, Industry, Academia, Local Government, Individual	NICCS Mapping Tool	88	\$52.59	\$4,628
<b>Total</b>		<b>1,688</b>		<b>\$88,775</b>

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 \$386,465. 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 \$90,962 (\$62,303 x 1.46 benefit multiplier = \$90,962)):

- Cost of NICSS SO to review NICCS Vetting Criteria Form: 2 personnel x 15% annual time = \$27,289
- Cost of NICCS SO to review NICCS Training Course Form: 2 personnel x 40% annual time = \$72,770

- Cost of NICCS SO to review NICCS Certification Course Form: 2 personnel x 15% annual time = \$27,289
- Cost of Training Catalog DBA: 100% annual time= ~\$90,962
- Cost of Training Catalog web developers: 3 personnel x 40% annual time = \$109,155
- Cost of server to host Training Catalog (recurring annually): = \$59,000

**Total: \$386,465**

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 revisions to the collection include:

- the addition of the NICCS Mapping Tool
- the updates to the Training Course Form
- Changing a form name from Vetting Criteria Form to Vendor Vetting Form
- Course Certification Form has been updated to be collected via email as a CSV file

DHS CE&A has revised the collection to include a new Mapping Tool form which will collect information to assist an end user with mapping his/her position description or position title to the new cybersecurity Framework 1.1 standard. Based on the addition of the tool, the public burden has increase by 350 number of responses, 88 burden hours and \$4,628 annual burden cost.

Also, DHS CE&A has revised the collection to make the Training Course Form a fully-electronic web form, and as a result of the fully electronic capabilities, the public burden has decreased by 30 minutes (.5 hours) per response, 525 burden hours, and \$27,610 annual burden cost.

The collection of the Course Certification Form via email is not expected to increase the burden estimates.

Based on all the collection updates, the total burden hours decreased by -437 total hours. The annual burden cost to respondents increased by \$1,777, from \$86,998 to \$88,775, due to updating the wage rate, but the increase was minimized due to the reduction in the burden for the Training Course Form. The annual government cost increased by \$23,243, from \$363,222 to \$386,465, due to updating the Federal wage rate.

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.

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 (<http://niccs.us-cert.gov/training/training-home>).

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.

DHS CE&A 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.

DHS CE&A does not request an exception to the certification of this information collection.