SUPPORTING STATEMENT FOR

Department of Homeland Security (DHS) Cybersecurity Education Office (CEO)
National Initiative for Cybersecurity Careers and Studies (NICCS)
Cybersecurity Training and Education Catalog (Training Catalog) Collection

OMB Control No.: 1601-NEW

COLLECTION INSTRUMENTS:

1. NICCS Cybersecurity Training Course Form
2. NICSS Cybersecurity Training Course Web Form (*to be developed*)
3. NICCS Vetting Criteria Form
4. NICCS Vetting Criteria Web Form (*to be developed*)
5. NICCS Certification Course Form
6. NICCS Certification Web Form (*to be developed*)

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.

Title II, Homeland Security Act, 6 U.S.C. §121(d)(1) To access, receive, and analyze laws enforcement information, intelligence information and other information from agencies of the Federal Government, State and local government agencies…and Private sector entities and to integrate such information in support of the mission responsibilities of the Department. The following authorities also permit DHS to collect information of the type contemplated: Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. §3546; Homeland Security Presidential Directive (HSPD) 7, "Critical Infrastructure Identification, Prioritization, and Protection" (2003); and NSPD-54/HSPD-23, "Cybersecurity Policy" (2009).

In May 2009, the President ordered a Cyberspace Policy Review to develop a comprehensive approach to secure and defend America's infrastructure. The review built upon the Comprehensive National Cybersecurity Initiative (CNCI).
In response to increased cyber threats across the Nation, the National Initiative for Cybersecurity Education (NICE) expanded from a previous effort, the CNCI #8. NICE formed in March 2011, and is a nationally coordinated effort comprised of over 20 federal departments and agencies, and numerous partners in academia and industry. NICE focuses on cybersecurity awareness, education, training and professional development. NICE seeks to encourage and build cybersecurity awareness and competency across the Nation and to develop an agile, highly skilled cybersecurity workforce.

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 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.

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 Office (CEO) intends for the collected information from the NICCS Cybersecurity Training Course Form and the NICCS Cybersecurity Certification Form to be displayed 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.

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

The DHS CEO NICCS Supervisory Office will use information collected from the NICCS Vetting Criteria Form to primarily manage communications with the training 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 Provider Form:
Organization Name and Address
Organization Point of Contact information (name, e-mail, phone number, etc.)
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 Signature.

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 completely collected via electronic means. Collection will be exchanged between the public and DHS CEO via e-mail (niccs@hq.dhs.gov).

All information collected from the NICCS Cybersecurity Training Course Form, 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://nics.us-cert.gov/training/training-home).

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

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 burden.

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 program or policy activities if the collection is not conducted or is conducted less frequently, as well as any technical or legal obstacles to reducing burden.

The Cybersecurity Training and Education Catalog exist solely to share cybersecurity training and education information with the general public, specifically for cybersecurity professionals. DHS CEO has identified the type of information and collection frequency in order to provide relevant, accurate, and timely information.

Transitioning from the NICCS Cybersecurity Training Course Form to the NICCS Cybersecurity Training Course Web Form will reduce the total annual respondent cost.

There are no legal obstacles.

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

- Requiring respondents to report information to the agency more often than quarterly;
- requiring respondents to prepare a written response to a collection of information in fewer than 30 days after receipt of it;

- requiring respondents to submit more than an original and two copies of any document;
- requiring respondents to retain records, other than health, medical, government contract, grant-in-aid, or tax records for more than three years;
- 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;
- requiring the use of a statistical data classification that has not been reviewed and approved by OMB;
- 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; or
- 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. If applicable, provide a copy and identify the data and page number of publication in the Federal Register of the agency's notice, required by 5 CFR 1320.8(d), 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.

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.

Consultation with representatives of those from whom information is to be obtained or those who must compile records should occur at least once every 3 years -- even if the collection of information activity is the same as in prior periods. There may be circumstances that may preclude consultation in a specific situation. These circumstances should be explained.

A 60 Day Federal Register Notice requesting public comments was published on Wednesday, June 12, 2013, 78 FR 35295. No comments were received.

A 30 Day Federal Register Notice requesting public comments was published on Thursday, September 19, 2013, 78 FR 57643. No comments were received.

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 covered by the existing Privacy Impact Assessment, DHS General Contact List (DHS/ALL/PIA-006) and the existing Systems of Records Notice, Department of Homeland Security (DHS) Mailing and other Lists Systems (DHS/ALL/SORN-002).

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 person's form 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:

- 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 desirable. 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.

- If this request for approval covers more than one form, provide separate hour burden estimates for each form and aggregate the hour burdens in Item 13 of OMB Form 83-I.

- Provide estimates of annualized cost to respondents for the hour burdens for collections of information, identifying and using appropriate wage rate categories. The cost of contracting out or paying outside parties for information collection activities should not be included here. Instead, this cost should be included in Item 14

Type of Respondent	Form Name / Form Number	No. Of Respondents	No. Of Responses per Respondent	Total Annual No. Of Responses	Avg. Burden per Response (in hours)	Total Annual Burden (in hours)	Avg. Hourly Wage Rate**	Total Annual Respondent Cost
Academic Institutions; Federal Government Organizations, Agencies, and Departments; Private Cybersecurity Training Providers	NICCS Cybersecurity Training Course Form	300	3	900	1	900	$29.24	$26,316
Academic Institutions; Federal Government Organizations, Agencies, and Departments; Private Cybersecurity Training Providers	NICCS Cybersecurity Training Course Web Form*	300	3	900	.5	450	$29.24	$11,808
Academic Institutions; Federal Government Organizations, Agencies, and Departments; Private Cybersecurity Training Providers	NICCS Certification Course Form	300	3	900	1	900	$29.24	$26,316
Academic Institutions; Federal Government Organizations, Agencies, and Departments; Private Cybersecurity Training Providers	NICCS Certification Course Web Form*	300	3	900	.5	450	$29.24	$13,158
Academic Institutions; Federal Government	NICCS Vetting	300	1	300	1	300	$29.24	$8,772

Organizations, Agencies, and Departments; Private Cybersecurity Training Providers	Criteria Form							
Academic Institutions; Federal Government Organizations, Agencies, and Departments; Private Cybersecurity Training Providers	NICCS Vetting Criteria Web Form*	300	1	300	.5	150	$29.24	$4,386
Total		900	7	2100 -Or- 1,050	3 -Or- 1.5	2,100 -Or- 1,050	$29.24	$6,404 -Or- $29,353

***Note 1**: *Online forms will replace their offline counterparts*.

****Note 2:** B*ased on the following Mean hourly wages (source: http://www.bls.gov/bls/blswage.htm):*

- *Educational Services, Privately owned - Computer and Mathematical Occupations - Information Security Analysts, Web Developers, and Computer Network Architects: $34.38*
- *Technical and trade schools, Privately owned - Information Security Analysts, Web Developers, and Computer Network Architects - $26.02*
- *Technical and trade schools, Local government owned - Network and Computer Systems Administrators - $26.00*
- *Technical and trade schools, State government owned - Network and Computer Systems Administrators - $25.10*
- *Colleges, universities, and professional schools, Privately owned - Information Security Analysts, Web Developers, and Computer Network Architects - $35.07*
- *Colleges, universities, and professional schools, Local government owned - Information Security Analysts, Web Developers, and Computer Network Architects - $28.54*
- *Colleges, universities, and professional schools, State government owned - Information Security Analysts, Web Developers, and Computer Network Architects - $29.57*

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).

- The cost estimate should be split into two components: (a) a total capital and start-up cost component (annualized over its expected useful life); and (b) a total operation and maintenance and purchase of services component. The estimates should take into account costs associated with generating, maintaining, and disclosing or providing the information. Include descriptions of methods used to estimate major cost factors including system and technology acquisition, expected useful life of capital equipment, the discount rate(s), and the time period over which costs will be incurred. Capital and start-up costs include, among other items, preparations for collecting information such as purchasing computers and software; monitoring, sampling, drilling and testing equipment; and record storage facilities.

- If cost estimates are expected to vary widely, agencies should present ranges of cost burdens and explain the reasons for the variance. The cost of purchasing or contracting out information collection services

should be a part of this cost burden estimate. In developing cost burden estimates, agencies may consult with a sample of respondents (fewer than 10), utilize the 60-day pre-OMB submission public comment process and use existing economic or regulatory impact analysis associated with the rulemaking containing the information collection, as appropriate.

- Generally, estimates should not include purchases of equipment or services, or portions thereof, made: (1) prior to October 1, 1995, (2) to achieve regulatory compliance with requirements not associated with the information collection, (3) for reasons other than to provide information or keep records for the government or (4) as part of customary and usual business or private practices.

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 not have been incurred without this collection of information. Agencies also may aggregate cost estimates from 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 $217,600. The following method was used to estimate the cost (based on General Schedule Grade 9, step 5, WASHINGTON-BALTIMORE-NORTHERN VIRGINIA, DC-MD-VA-WV-PA locality, annual pay):

- Cost of NICSS SO to review NICCS Vetting Criteria Form: 2 personnel x 15% annual time = $17,550
- Cost of NICCS SO to review NICCS Training Course Form: 2 personnel x 40% annual time = $46,800
- Cost of NICCS SO to review NICCS Certification Course Form: 2 personnel x 15% annual time = $17,550
- Cost of Training Catalog DBA: 100% annual time= ~$58,500
- Cost of Training Catalog web developers: 3 personnel x 40% annual time = $70,200
- Cost of server to host Training Catalog: = $7000

Total:

- $217,600 initial;
- $210,600 subsequent years (minus the initial cost of server).

15. Explain the reasons for any program changes or adjustments reporting in Items 13 or 14 of the OMB Form 83-I.

This is a new collection; therefore, there has been no increase or decrease in the estimated annual burden hours previously reported for this information collection.

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 the NICCS Cybersecurity Training Course Form, NICCS Cybersecurity Training Course Web Form, and the NICCS Certification Couse Form will be stored in the publicly accessible NICCS Cybersecurity Training and Education Catalog (http://nics.us-cert.gov/training/training-home).

No complex analytical techniques will be used.

Information will be published to the NICCS Cybersecurity Training and Education Catalog three times a calendar year: February 6, April 24, and July 24.

This project has no set end date.

Collection of information will commence upon official collection approval.

Information collected using the NICCS Vetting Criteria Form will not be published or otherwise made publicly available.

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

DHS CEO 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 Submission," of OMB 83-I.

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