9110-9B

DEPARTMENT OF HOMELAND SECURITY

Agency Information Collection Activities**:** 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

AGENCY: Cybersecurity Education Office, DHS

ACTION: 60-Day Notice and request for comments; New Collection (Request for a new OMB Control No.), 1601-NEW

SUMMARY: The Department of Homeland Security, Cybersecurity Education Office, will submit the following Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995 (P.L. 104-13, 44 U.S.C. Chapter 35).

DATES: Comments are encouraged and will be accepted until [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This process is conducted in accordance with 5 CFR 1320.1

ADDRESSES: Written comments and questions about this Information Collection Request should be forwarded to Cybersecurity Education Office , DHS Attn.: Michael Wigal, dhs.pra@hq.dhs.gov

SUPPLEMENTARY INFORMATION: Title II, Homeland Security Act, 6 U.S.C. §121(d)(1) To access, receive, and analyze law 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. Both

Training Course and Certification information will be stored 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 (SO).

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 the NICCS Cybersecurity Training Course Form and the NICCS Cybersecurity Certification Form will be included in the Cybersecurity Training and Education Catalog. Both sets of information will be made available to the public to support the National Initiative for Cybersecurity Education (NICE) mission and the Comprehensive National Cybersecurity Initiative (CNCI) – Initiative 8: Expand Cyber Education.

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 and certification owners before uploading their training course or certification

information to the Training Catalog.

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

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

The Office of Management and Budget is particularly interested in comments which:

1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;
2. Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;
3. Enhance the quality, utility, and clarity of the information to be collected; and
4. Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic,

mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submissions of responses.

ANALYSIS:

AGENCY: Cybersecurity Education Office, DHS

Title: 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 Number: 1601-NEW

Number of Respondents: 300

Estimated Number of Responses: 2100

Estimated Time Per Respondent: 1 hour

Total Burden Hours: 2100 hours

Dated: June 4, 2013

Margaret H. Graves
Acting Chief Information Officer.

[FR Doc. 2013-13885 Filed 06/11/2013 at 8:45 am; Publication Date: 06/12/2013]