DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA-2024-0016]

Agency Information Collection Activities: National Initiative for Cybersecurity Careers and Studies Cybersecurity Education and Training Catalog Collection

AGENCY: Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS).

ACTION: 60-day notice and request for comments; revised information collection request: 1670–0030.

SUMMARY: NICCS within CISA will submit the following Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review and clearance.

DATES: Comments are encouraged and will be accepted until ***[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]***. Submissions received after the deadline for receiving comments may not be considered.

ADDRESSES: You may submit comments, identified by docket number CISA-2024-0016, at: Federal eRulemaking Portal: http://www.regulations.gov. Please follow the instructions for submitting comments.

Instructions: All submissions received must include the agency name and docket number CISA-2024-0016. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FUTHER INFORMATION CONTACT: Shannon Nguyen, 703-705-6246, shannon.nguyen@cisa.dhs.gov.

SUPPLEMENTARY 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.

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:

CISA OCLO seeks to utilize four separate forms in 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 a publicly accessible website called the National Initiative for Cybersecurity Careers and Studies (NICCS) website (https://niccs.cisa.gov). Collected information from these two forms will be included in the Cybersecurity Training and Education Catalog that is hosted on the NICCS website. Requested information categories in these forms include the training providers name, course title, course description, course length, course modality, among other course information useful for users.

The 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. Requested information in the NICCS Vendor Vetting form include vendor name, address, points of contact and a few multiple-choice questions to ensure they are a legitimate business.

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. This collected information will not be shared with the public and is intended for internal use only. Requested information in the NICCS Mapping form include: Selecting various work roles (based on the NICE Framework), selecting tasks required for that work role, and including job description details.

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.

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.

ANALYSIS:

AGENCY: Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS)

Title: National Initiative for Cybersecurity Careers and Studies Cybersecurity Education and Training Catalog Collection.

OMB Number: 1670–0030.

Frequency: Annually.

Affected Public: General Public.

Number of Respondents: 500.

Estimated Time Per Respondent: 0.775 Hours.

Total Burden Hours: 387.5.

Annualized Respondent Cost: $24,482.

Total Annualized Respondent Out-of-Pocket Cost: $0.

Total Annualized Government Cost: $161,490.

Robert J. Costello,
Chief Information Officer,
Department of Homeland Security,
Cybersecurity and Infrastructure Security Agency.

[FR Doc. 2024-13471 Filed: 6/18/2024 8:45 am; Publication Date: 6/20/2024]