its continuing effort to reduce paperwork and respondent burden, invites the general public to take this opportunity to comment on a reinstatement, with change, of a previously approved information collection for which approval has expired. FEMA will submit the information collection abstracted below to the Office of Management and Budget (OMB) for review and clearance in accordance with the requirements of the Paperwork Reduction Act of 1995. The submission will describe the nature of the information collection, the categories of respondents, the estimated burden (*i.e.,* the time, effort and resources used by respondents to respond) and cost, and the actual data collection instruments FEMA will use.

DATES: Comments must be submitted on or before November 4, 2022.

ADDRESSES: Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to *www.reginfo.gov/public/do/PRAMain.* Find this particular information collection by selecting ''Currently under 30-day Review—Open for Public Comments'' or by using the search function.

FOR FURTHER INFORMATION CONTACT: Requests for additional information or copies of the information collection should be made to Director, Information Management Division, 500 C Street SW, Washington, DC 20472, email address *FEMA-Information-Collections-Management@fema.dhs.gov* or Joycelyn Collins, Underwriting Branch Program Analyst, Federal Insurance Directorate, 202–701–3383.

SUPPLEMENTARY INFORMATION: The NFIP is authorized by Public Law 90–448 (1968) and expanded by Public Law 93–234 (1973). The National Flood Insurance Act of 1968 requires that FEMA provide flood insurance at full actuarial rates reflecting the complete flood risk to structures built or substantially improved on or after the effective date for the initial Flood Insurance Rate Map for the community, or after December 31, 1974, whichever is later, so that the risks associated with buildings in flood-prone areas are borne by those located in such areas and not by the taxpayers at large. In accordance with Public Law 93–234, the purchase of flood insurance is mandatory when Federal or federally-related financial assistance is being provided for acquisition or construction of buildings located, or to be located, within FEMA-identified special flood hazard areas of communities that participate in the NFIP.

This proposed information collection previously published in the **Federal Register** on December 16, 2020 at 85 FR 81481 with a 60-day public comment period. No comments were received. This information collection expired on April 30, 2020. FEMA is requesting a reinstatement, with change, of a previously approved information collection for which approval has expired. The purpose of this notice is to notify the public that FEMA will submit the information collection abstracted below to the Office of Management and Budget for review and clearance.

Collection of Information

Title: National Flood Insurance Program Policy Forms.

Type of information collection: Reinstatement, with change, of a previously approved collection for which approval has expired.

OMB Number: 1660–0006.

Form Titles and Numbers: FEMA Forms 086–0–1 and 086–0–1T, Flood Insurance Application; FEMA Forms 086–0–2 and 086–0–2T, Flood Insurance Cancellation/Nullification Request Form; FEMA Forms 086–0–3 and 086–3T, Flood Insurance General Change Endorsement; FEMA Form 086–0–4, V-Zone Risk Factor Rating Form and Instructions (discontinued October 16, 2019, due to insufficient use); and FEMA Form 086–0–5T, Flood Insurance Preferred Risk Policy and Newly Mapped Application.

Abstract: To provide for the availability of policies for flood insurance, policies are marketed and administered through the facilities of licensed insurance agents or brokers in the various states. Applications, general change requests, and cancellations from agents or brokers are forwarded to a direct servicing agent designated as fiscal agent by the Federal Insurance and Mitigation Administration, referred to as NFIP Direct. Upon receipt and examination of the application, general change request, cancellation, and required premium, the servicing company issues or updates the appropriate Federal flood insurance policy.

Affected Public: Individuals or households; State, Local or Tribal Government; Business or other for profit; Not-for-profit institutions; and Farms.

Estimated Number of Respondents: 409,781.

Estimated Number of Responses: 409,781.

Estimated Total Annual Burden Hours: 62,196.

Estimated Total Annual Respondent Cost: $2,335,459.

Estimated Respondents' Operation and Maintenance Costs: $0.

Estimated Respondents' Capital and Start-Up Costs: $0.

Estimated Total Annual Cost to the Federal Government: $9,360,407.

Comments

Comments may be submitted as indicated in the **ADDRESSES** caption above. Comments are solicited to (a) evaluate whether the proposed data collection is necessary for the proper performance of the agency, including whether the information shall have practical utility; (b) 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; (c) enhance the quality, utility, and clarity of the information to be collected; and (d) 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 submission of responses.

Millicent L. Brown,

Senior Manager, Records Management Branch, Office of the Chief Administrative Officer, Mission Support, Federal Emergency Management Agency, Department of Homeland Security.

[FR Doc. 2021–06875 Filed 4–2–21; 8:45 am]

BILLING CODE 9111–52–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2021–0004]

Privacy Act of 1974; System of Records

AGENCY: Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security.

ACTION: Notice of a New System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the U.S. Department of Homeland Security (DHS) proposes to establish a new DHS system of records titled, ''DHS/Cybersecurity and Infrastructure Security Agency (CISA)–005 Administrative Subpoenas for Cybersecurity Vulnerability Identification and Notification System of Records.'' This system of records allows DHS/CISA (''Agency'') to receive and collect customer or subscriber contact information from electronic communications service providers to

identify and notify entities at risk of security vulnerabilities relating to critical infrastructure information systems and devices. This newly established system will be included in DHS's inventory of record systems.

DATES: Submit comments on or before May 5, 2021. This new system will be effective upon publication. Routine uses will be effective May 5, 2021.

ADDRESSES: You may submit comments, identified by docket number CISA–2021–0004 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov*. Follow the instructions for submitting comments.
- *Fax:* 202–343–4010.
- *Mail:* Lynn Parker Dupree, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528–0655.

Instructions: All submissions received must include the agency name and docket number CISA–2021–0004. 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 FURTHER INFORMATION CONTACT: For general questions, please contact: James Burd, (703) 235–1919, *Privacy@cisa.dhs.gov,* Chief Privacy Officer, Office of the Privacy Office, Cybersecurity and Infrastructure Security Agency, Washington, DC 20528–0655. For privacy questions, please contact: Lynn Parker Dupree, (202) 343–1717, *Privacy@hq.dhs.gov,* Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528–0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) proposes to establish a new CISA system of records entitled, ''DHS/CISA—Administrative Subpoenas for Cybersecurity Vulnerability Identification System of Records.'' Subsection (o) of Section 2209 of the Homeland Security Act, as amended, 6 U.S.C. 659(o), grants CISA the authority to issue a subpoena for the production of information necessary to identify and notify an entity at risk, where the entity owns or operates what CISA has reason to believe is a ''covered device or system'' [1] with a specific security vulnerability relating to critical infrastructure, and if CISA itself is unable to identify the entity at risk that owns or operates such covered device or system. CISA will issue subpoenas to providers of public electronic communications services, such as Internet Service Providers (ISP), that have relevant customer or subscriber information to identify the owners or operators of covered devices or systems with a specific security vulnerability, often identified through their internet protocol (IP) address. The Electronic Communications Privacy Act of 1986 (18 U.S.C. 2510 *et seq*.) permits the federal government to subpoena such service providers for basic subscriber information. The information to be collected by CISA is not for intelligence or prosecution activities, but rather to notify entities of potential cybersecurity risks to covered devices or systems with a specific security vulnerability relating to critical infrastructure.

This system of records will cover records of individuals identified in the information provided by the ISP as the owner or operator of a covered device or system connected to the internet with a specific security vulnerability related to critical infrastructure. CISA maintains this information to identify and notify the individual of the vulnerability on the covered device or system.[2]

This newly established system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which federal government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a ''system of records.'' A ''system of records'' is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, the Judicial Redress Act (JRA) provides covered persons with a statutory right to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/CISA–005 Administrative Subpoenas for Cybersecurity Vulnerability Identification and Notification System of Records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER:

DHS/CISA–005 Administrative Subpoenas for Cybersecurity Vulnerability Identification and Notification.

SECURITY CLASSIFICATION:

Controlled Unclassified Information.

SYSTEM LOCATION:

Records are maintained at CISA locations such as Arlington, Virginia and Pensacola, Florida.

SYSTEM MANAGER(S):

Division Director, National Cybersecurity and Communications Integration Center (NCCIC) Hunt & Incident Response, 1110 North Glebe Rd. Arlington, VA 22201.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Subsection (o) of Section 2209 of the Homeland Security Act, as amended, 6 U.S.C. 659(o).

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is to maintain records for the purpose of identifying and notifying entities at risk of security vulnerabilities relating to critical infrastructure on covered devices and systems. The authority is available only in circumstances where CISA knows of a specific cybersecurity risk to a covered device or system but is unable to determine the owner or operator of the covered device or system. The information sought by subpoena is limited to only basic categories of subscriber information.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individual(s) whose contact information is provided by an electronic

[1] ''Covered device or system'' means a device or system commonly used to perform industrial, commercial, scientific, or government functions or processes related to critical infrastructure, including operational and industrial control systems, distributed control systems, and programmable logic controllers. The term ''covered device or system'' does not include personal devices or systems, such as consumer mobile devices, home computers, residential wireless routers, or residential internet enabled consumer devices. *See* 6 U.S.C. 659(o)(1).

[2] Pursuant to 6 U.S.C. 659(o)(8), the Agency may not require an owner or operator of critical infrastructure to take any action as a result of a notice of vulnerability made pursuant to 6 U.S.C. 659(o).

communication service provider in response to a subpoena as described above.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system include the following information obtained through subpoenas:

- Name;
- Address;
- Length of service (including start date) and types of service utilized; and
- Telephone or instrument number or other subscriber number or identity.

In addition, the system will also include the following categories of records:

- IP address;
- Individual's position/title or organizational affiliations; and
- Identifier or ticket number created by CISA to retrieve information.

RECORD SOURCE CATEGORIES:

Information is obtained from a subpoenaed individual, partnership, corporation, association, or entity. Information may also be obtained through public sources or contact with an individual identified through the issuing of a subpoena.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

In accordance with subsection (o) of Section 2209 of the Homeland Security Act, as amended, (6 U.S.C. 659(o)), the Agency may not disseminate nonpublic information obtained through a subpoena that identifies the party that is subject to such subpoena or the entity at risk identified by information obtained, except that the Agency may share the nonpublic information with the Department of Justice for the purpose of enforcing such subpoena in non-compliance circumstances, and may share with a federal agency the nonpublic information of the entity at risk if the requirements of 6 U.S.C. 659(o)(7)(A) are met so long it is used by that federal agency for a cybersecurity purpose, as defined in 6 U.S.C. 1501, in accordance with 6 U.S.C. 659(o)(12).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

CISA will retrieve records by CISA-created ticket number associated with a covered device or system connected to the internet identified as having a security vulnerability. Records may also be retrieved by IP address or phone number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records that are stored in an individual's file will be purged according to the retention and disposition guidelines under 6 U.S.C. 659(o)(7)(C)(ii), which requires destruction of any personally identifiable information not later than six (6) months after the date on which the Agency receives information obtained through subpoena, unless otherwise agreed to by the individual identified by the subpoena respondent. CISA is developing a records retention schedule for submission and approval by the National Archives Records Administration.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

CISA safeguards records in this system according to applicable rules and policies, including all applicable CISA automated systems security and access policies. CISA has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those CISA officials who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES:

Individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the DHS Chief Privacy Officer or the appropriate Headquarters or component's FOIA Officer whose contact information can be found at *https://www.dhs.gov/freedom-information-act-foia* under ''Contact Information.'' If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the DHS Chief Privacy Officer and Chief Freedom of Information Act Officer, U.S. Department of Homeland Security, Washington, DC 20528–0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about you may be available under the Freedom of Information Act.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign the request, and the individual's signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. In addition, the individual should:

- Explain why he or she believes the Department would have information being requested;
- Identify which component(s) of the Department he or she believes may have the information;
- Specify when the individual believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records.

If the request is seeking records pertaining to another living individual, the request must include an authorization from the individual whose record is being requested, authorizing the release to the requester.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES:

For records covered by the Privacy Act, individuals may make a request for amendment or correction of a record of the Department about the individual by writing directly to the Department component that maintains the record, unless the record is not subject to amendment or correction. The request should identify each particular record in question, state the amendment or correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The individual may submit any documentation that would be helpful. If the individual believes that the same record is in more than one system of records, the request should state that and be addressed to each component that maintains a system of records containing the record.

NOTIFICATION PROCEDURES:

See ''Record Access Procedures'' above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

* * * * *

Lynn Parker Dupree,

Chief Privacy Officer, U.S. Department of Homeland Security.

[FR Doc. 2021–06874 Filed 4–2–21; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

U.S. Immigration and Customs Enforcement

[OMB Control Number 1653–0054]

Agency Information Collection Activities; Extension, Without Change, of a Currently Approved Collection: Training Plan for Science, Technology, Engineering, and Mathematics (STEM) Optional Practical Training (OPT) Students

AGENCY: U.S. Immigration and Customs Enforcement, Department of Homeland Security.

ACTION: 60-Day notice.

SUMMARY: In accordance with the Paperwork Reduction Act (PRA) of 1995, U.S. Immigration and Customs Enforcement (ICE), the Department of Homeland Security (DHS), 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 June 4, 2021.

ADDRESSES: All submissions received must include the OMB Control Number 1653–0054 in the body of the correspondence, the agency name and Docket ID ICEB–2018–0003–0001. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.

(1) *Online.* Submit comments via the Federal eRulemaking Portal website at *http://www.regulations.gov* under e-Docket ID number ICEB–2018–0003–0001.

FOR FURTHER INFORMATION CONTACT: If you have questions related to this collection, call or email Sharon Snyder, Student and Exchange Visitor Program (SEVP), 703–603–3400 or 1–800–892–4829, email: *sevp@ice.dhs.gov.*

SUPPLEMENTARY INFORMATION:

Comments

Written comments and suggestions from the public and affected agencies concerning the proposed collection of information should address one or more of the following four points:

(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 submission of responses.

Overview of This Information Collection

(1) *Type of Information Collection:* Extension, Without Change, of a Currently Approved Collection.

(2) *Title of the Form/Collection:* Training Plan for STEM OPT Students.

(3) *Agency form number, if any, and the applicable component of the Department of Homeland Security sponsoring the collection:* Form I–983; U.S. Immigration and Customs Enforcement.

(4) *Affected public who will be asked or required to respond, as well as a brief abstract:* Primary: Individuals or households. The Form I–983 serves as a planning document for STEM OPT students, the SEVP-certified school officials, and the employers. The Training Plan for STEM OPT Students also serves as an evidentiary document for SEVP, by tracking the STEM OPT student's progress, setting forth the terms and conditions of the practical training, and documenting the obligations of the three parties that are involved—the F student, the SEVP-certified school, and the employer.

The student and the employer must each complete and sign their part of the Form I–983. The SEVP-certified school will incorporate the completed and signed Form I–983 as part of the student's school file. The SEVP-certified school will make the student's Form I–983 available to DHS upon request.

(5) *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:*

TABLE 1—CALCULATION OF ANNUAL REPORTING BURDEN FOR TRAINING PLAN

Function	Avg. annual responses	Time per response (hours)	Avg. annual hour burden [1]
Student Burden			
Initial Completion of Training Plan	66,565	2.17	144,446
12-month Evaluation Requirements	66,565	1.50	99,848
Subtotal	.....	.....	244,294
DSO Burden			
Initial Review of Training Plan & Recordkeeping	66,565	1.33	88,531
Review of Evaluation & Recordkeeping	66,565	1.33	88,531
Subtotal	.....	.....	177,062
Employer Burden			
Initial Completion of Training Plan	66,565	4.00	266,260
Evaluation Requirements	66,565	0.75	49,924