agree with one or more non-Federal parties to share research resources, but the Federal party does not contribute funding.

CRADAs are not procurement contracts. Care is taken to ensure that CRADAs are not used to circumvent the contracting process. CRADAs have a specific purpose and should not be confused with procurement contracts, grants, and other type of agreements.

Under the proposed CRADA, the Coast Guard's Research and Development Center (R&DC) will collaborate with one or more non-Federal participants. Together, the R&DC and the non-Federal participants will evaluate SUAS and their airborne sensors to determine their potential for use in a maritime environment by a first responder and DHS operational components.

We anticipate that the Coast Guard's contributions under the proposed CRADA will include the following:

(1) Develop the demonstration test plan to be executed under the CRADA;

(2) Provide the SUAS test range, test range support, facilities, and all approvals required for a 5 day demonstration under the CRADA;

(3) Conduct the privacy threshold analysis required for the demonstration;

(4) Conduct the privacy impact assessment required for the demonstration;

(5) Coordinate any required spectrum approval for the SUAS;

(6) Coordinate and receive any required interim flight clearance for the demonstration;

(7) Provide any required airspace coordination and de-confliction for the demonstration test plan;

(8) Collect and analyze demonstration test plan data; and

(9) Develop a demonstration final report documenting the methodologies, findings, conclusions, and recommendations of this CRADA work.

We anticipate that the non-Federal participants' contributions under the proposed CRADA will include the following:

(1) Provide SUAS and all other equipment to conduct the demonstration described in the demonstration test plan;

(2) Provide all required operators and technicians to conduct the demonstration;

(3) Provide technical data for the SUAS to be utilized;

(4) Provide shipment and delivery of all SUAS equipment required for the demonstration; and

(5) Provide travel and associated personnel and other expenses as required.

The Coast Guard reserves the right to select for CRADA participants all, some, or no proposals submitted for this CRADA. The Coast Guard will provide no funding for reimbursement of proposal development costs. Proposals and any other material submitted in response to this notice will not be returned. Proposals submitted are expected to be unclassified and have no more than five single-sided pages (excluding cover page, DD 1494, JF–12, etc.). The Coast Guard will select proposals at its sole discretion on the basis of:

(1) How well they communicate an understanding of, and ability to meet, the proposed CRADA's goal; and

(2) How well they address the following criteria:

(a) Technical capability to support the non-Federal party contributions described; and

(b) Resources available for supporting the non-Federal party contributions described.

Currently, the Coast Guard is considering AeroVironment, Inc. for participation in this CRADA, because they have demonstrated the ability to operate SUAS in a maritime environment. However, we do not wish to exclude other viable participants from this or future similar CRADAs.

This is a technology demonstration effort. The goal of this CRADA is to identify and investigate the potential of the SUAS and their airborne sensors to determine their potential use in a maritime environment by the first responder and the DHS operational components. Special consideration will be given to small business firms/consortia, and preference will be given to business units located in the U.S.

This notice is issued under the authority of 5 U.S.C. 552(a) and 15 U.S.C. 3710(a).

Dated: November 2, 2017.

Gregory C. Rothrock,

Captain, USCG, Commanding Officer, U.S. Coast Guard Research and Development Center.

[FR Doc. 2017–25076 Filed 11–17–17; 8:45 am]

BILLING CODE 9110–04–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2017–0048]

The Department of Homeland Security, National Protection and Programs Directorate, National Initiative for Cybersecurity Careers and Studies Cybersecurity Training and Education Catalog Collection

AGENCY: National Protection and Programs Directorate (NPPD), Department of Homeland Security (DHS).

ACTION: 60-day notice and request for comments; Revised Information Collection Request: 1670–0030.

SUMMARY: The DHS NPPD Office of Cybersecurity & Communications (CS&C), Cybersecurity Education & Awareness Office (CE&A), National Initiative for Cybersecurity Careers and Studies (NICCS) will submit the following Information Collection Request to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995.

DATES: Comments are encouraged and will be accepted until January 19, 2018. This process is conducted in accordance with 5 CFR part 1320.

ADDRESSES: Comments must be identified by ''DHS–2017–0048'' and may be submitted by *one* of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.*
- *Email: niccs@hq.dhs.gov.* Include the docket number ''DHS–2017–0048'' in the subject line of the message.
- *Mail:* Written comments and questions about this Information Collection Request should be forwarded to DHS/NPPD 245 Murray Lane SW., Mailstop 0380, Arlington, VA 20598–0380.

Instructions: All submissions received must include the words ''Department of Homeland Security'' and docket number ''DHS–2017–0048''. Comments received will be posted without alteration at *http://www.regulations.gov,* including any personal information provided. Written comments should reach the contact person listed no later than January 19, 2018.

FOR FURTHER INFORMATION CONTACT: For specific questions related to collection activities, please contact Shannon Nguyen at 703–705–6246 or at *niccs@hq.dhs.gov.*

SUPPLEMENTARY INFORMATION: Title II of the Homeland Security Act of 2002, 6 U.S.C. 121(d)(1), says that the Secretary of Homeland Security has the

responsibility ''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 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.

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 email the NICCS Supervisory 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 Web site 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.

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.

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 collected information will not be shared with the public and is intended for internal use only.

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 email (*niccs@hq.dhs.gov*).

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.

OMB is particularly interested in comments that:

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.

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

OMB Number: 1670–0030.

Frequency: Occassionally.

Affected Public: Educational Institutes (Privately Owned, and State/Local Government Owned).

Number of Respondents: 1,350 respondents.

Estimated Time per Respondent: 30 minutes.

Total Burden Hours: 1,688 annual burden hours.

Total Burden Cost: $0.

Total Recordkeeping Burden: $0.

Scott Libby,

Deputy Chief Information Officer.

[FR Doc. 2017–25102 Filed 11–17–17; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF THE INTERIOR

Bureau of Land Management

[LLMT926000 L19100000.BK0000 LRCSEX702500; 18XL1109AF; MO# 4500115885]

Notice of Proposed Filing of Plats of Survey: Montana

AGENCY: Bureau of Land Management (BLM), Interior.

ACTION: Notice of proposed official filing.

SUMMARY: The plats of surveys for the lands described in this notice are scheduled to be officially filed 30 calendar days after the date of this publication in the BLM Montana State Office, Billings, Montana. The surveys, which were executed at the request of the Bureau of Indian Affairs, Rocky Mountain Region, Billings, Montana, are necessary for the management of these lands.

DATES: A person or party who wishes to protest this decision must file a notice of protest in time for it to be received in the BLM Montana State Office no later than 30 days after the date of this publication.

ADDRESSES: A copy of the plats may be obtained from the Public Room at the BLM Montana State Office, 5001 Southgate Drive, Billings, Montana 59101, upon required payment. The plats may be viewed at this location at no cost.

FOR FURTHER INFORMATION CONTACT: Josh Alexander, BLM Chief Cadastral Surveyor for Montana; telephone: (406) 896–5123; email: *jalexand@blm.gov.* Persons who use a telecommunications device for the deaf (TDD) may call the Federal Relay Service (FRS) at (800) 877–8339 to contact the above individual during normal business hours. The FRS is available 24 hours a day, 7 days a week, to leave a message or question with the above individual. You will receive a reply during normal business hours.

SUPPLEMENTARY INFORMATION: The lands surveyed are: