DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket Number USCG–2024–0339]

Cooperative Research and Development Agreement: Incident Driven Video Recording Systems (IDVRS) in the Form of Body-Worn Cameras (BWC), Various Accessories, Docking Stations, Video Management System (VMS) Software, and Cloud Storage Technology

AGENCY: Coast Guard, DHS.

ACTION: Notice of intent; request for comments.

SUMMARY: The Coast Guard is announcing its intent to enter into a Cooperative Research and Development Agreement (CRADA) with Axon Enterprise, Inc. to evaluate Incident Driven Video Recording Systems (IDVRS) in the form of body-worn cameras (BWC), various accessories, docking stations, video management system (VMS) software, and cloud storage technology. While the Coast Guard is currently considering partnering with Axon Enterprise, Inc., we are soliciting public comment on the possible nature of and participation of other parties in the proposed CRADA. In addition, the Coast Guard also invites other potential Federal participants, who have the interest and capability to bring similar contributions to this type of research, to consider submitting proposals for consideration in similar CRADAs.

DATES: Your comments and related material must reach the Coast Guard on or before July 26, 2024.

ADDRESSES: You may submit comments identified by docket number USCG–2024–0339 using the Federal portal at *https://www.regulations.gov.* See the ''Public Participation and Request for Comments'' portion of the **SUPPLEMENTARY INFORMATION** section for further instructions on submitting comments.

FOR FURTHER INFORMATION CONTACT: If you have questions about this notice of intent, call or email Matt Burton, Rapid Reaction Technology Branch, U.S. Coast Guard Research and Development Center; telephone 860–271–2600, email *rdc-info@uscg.mil.*

SUPPLEMENTARY INFORMATION:

I. Table of Abbreviations

BWC Body-worn cameras
CRADA Cooperative Research and Development Agreement
DHS Department of Homeland Security
LEOs Law enforcement officers
U.S.C. United States Code

II. Background and Purpose

The Coast Guard is developing a material solution to meet the requirements for body-worn cameras (BWC) as specified in Executive Order 14074 of May 25, 2022, and DHS's BWC Policy 045–47 (2023). The BWC policy mandates the use of body cameras for Law Enforcement Officer's (LEO's) while engaged in interactions with the public, pre-planned arrest warrants, and during the execution of search and seizure warrants or orders. The BWC program has limited implementation within the Coast Guard and is currently utilized by select operational units on a small scale. The Research and Development Center is supporting a technology understanding of the Coast Guard's interest in expanding BWC usage to all LEO's.

III. Public Participation and Request for Comments

We request public comments on this notice. Although we do not plan to respond to comments in the **Federal Register**, we will respond directly to commenters and may modify our proposal in light of comments.

We encourage you to submit comments in response to this notice of inquiry through the Federal Decision Making portal at *https://www.regulations.gov.* To do so, go to *https://www.regulations.gov,* type USCG–2024–0339 in the search box and click ''Search.'' Next, look for this document in the Search Results column, and click on it. Then click on the Comment option. In your submission, please include the docket number for this notice of inquiry and provide a reason for each suggestion or recommendation. If your material cannot be submitted using *https://www.regulations.gov,* contact the person in the **FOR FURTHER INFORMATION CONTACT** section of this document for alternate instructions. Public comments will also be placed in our online docket and can be viewed by following instructions on the *https://www.regulations.gov* Frequently Asked Questions web page. We review all comments received, but we may choose not to post off-topic, inappropriate, or duplicate comments that we receive.

We accept anonymous comments. Comments we post to *https://www.regulations.gov* will include any personal information you have provided. For more about privacy and submissions in response to this document, see DHS's eRulemaking System of Records notice (85 FR 14226, March 11, 2020).

IV. Discussion

Cooperative Research and Development Agreements (CRADAs) are authorized under 15 U.S.C. 3710a.[1] A CRADA promotes the transfer of technology to the private sector for commercial use, as well as specified research or development efforts that are consistent with the mission of the Federal parties to the CRADA. The Federal party or parties 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 R&D Center will collaborate with one non-Federal participant. Together, the R&D Center and the non-Federal participant will conduct an evaluation of the BWC technology and support systems in various test scenarios to determine the technology's performance and suitability to Coast Guard LEO missions.

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

1. Provide appropriate staff with pertinent expertise to take the lead in accomplishing the required tasks;
2. Provide information regarding the ensemble items and parameters needed for creating the test plan;
3. Provide all support resources, including travel, for Coast Guard staff that supports this CRADA;
4. Obtain, transport and provide all of the ensemble items to be used during the testing;
5. Provide personnel support to non-Federal participant to assist with setting up and execute testing in accordance with the agreed upon test plan; and
6. Work with non-Federal participant to develop a Final Report, which will document 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 appropriate staff with pertinent expertise to support the above mentioned tasks;

[1] The statute confers this authority on the head of each Federal agency. The Secretary of DHS's authority is delegated to the Coast Guard and other DHS organizational elements by DHS Delegation No. 0160.1, para. II.B.34.

2. Provide necessary technology equipment and services needed to conduct test scenarios;

3. Provide technical assistance for the test plan;

4. Provide support services during the Coast Guard's test scenarios in accordance with the agreed upon test plan; and

5. Provide test data review and feedback as agreed upon completion of testing.

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 not 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 Axon Enterprise, Inc. for participation in this CRADA. This consideration is based on the fact that Axon Enterprise, Inc. has demonstrated its technical capability and ability to comply with DHS and DoD requirements for BWC implementation. However, we do not wish to exclude other viable participants from this or similar CRADAs in the future.

This is a technology evaluation effort. The goal of this CRADA is to evaluate technology for its potential compatibility, integration, and ease of use with Coast Guard uniforms, Personal Protective Equipment (PPE), and enforcement gear used by Coast Guard personnel as well as the compatibility, integration, and ease of use with Coast Guard Information Technology (IT) systems. Special consideration will be given to small business firms and 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).

Dated: June 20, 2024.

M.P. Chien,

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

[FR Doc. 2024–13927 Filed 6–25–24; 8:45 am]

BILLING CODE 9110–04–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2024–0013]

Agency Information Collection Activities: Incident Reporting Form and Associated Submission Tools (ICR 1670–0037)

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

ACTION: 60-Day notice and request for comments.

SUMMARY: DHS CISA Cybersecurity Division (CSD) submits the following Information Collection Request (ICR) renewal 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 August 26, 2024.

ADDRESSES: You may submit comments, identified by docket number CISA–2024–0013 at;

- *Federal eRulemaking Portal: http://www.regulations.gov.* Please follow the instructions for submitting comments.

Instructions: All submissions received must include the words ''Department of Homeland Security'' and the docket number for this action. Comments received will be posted without alternation to *http://www.regulations.gov,* including any personal information provided.

Docket: For access to the docket to read background documents or comments received, please go to *http://www.regulations.gov* and enter docket number CISA–2024–0013.

Comments submitted in response to this notice may be made available to the public through relevant websites. For this reason, please do not include in your comments information of a confidential nature, such as sensitive personal information or proprietary information. If you send an email comment, your email address will be automatically captured and included as part of the comment that is placed in the public docket and made available on the internet. Please note that responses to this public comment request containing any routine notice about the confidentiality of the communication will be treated as public comments that may be made available to the public notwithstanding the inclusion of the routine notice.

FOR FURTHER INFORMATION CONTACT: Brian DeWyngaert; 703–235–5737; *Brian.dewyngaert@cisa.dhs.gov.*

SUPPLEMENTARY INFORMATION: CISA serves as ''a Federal civilian interface for the multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities.'' 6 U.S.C. 659(c)(1).

CISA is responsible for performing, coordinating, and supporting response to information security incidents, which may originate outside the Federal community and affect users within it, or originate within the Federal community and affect users outside of it. CISA uses the information from incident reports to develop timely and actionable information for distribution to federal departments and agencies; state, local, tribal and territorial (SLTT) governments; critical infrastructure owners and operators; private industry; and international organizations. Often, the effective handling of security incidents relies on information sharing among individual users, industry, and the Federal Government, which may be facilitated by and through CISA.

Pursuant to the *Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. 3552 et seq.*, CISA operates the federal information security incident center for the United States Federal Government. 44 U.S.C. 3556. Federal agencies notify and consult with CISA regarding information security incidents involving federal information systems. CISA provides federal agencies with technical assistance and guidance on detecting and handling security incidents, compile and analyze incident information that threatens information security, inform agencies of current and potential threats and vulnerabilities, and provide intelligence or other information about cyber threats, vulnerabilities, and incidents to agencies. 44 U.S.C. 3556(a). CISA also receives voluntary incident reports from non-federal entities.

CISA's website (at *https://www.cisa.gov/*) is a primary tool used by constituents to report incident information, access information sharing products and services, and interact with CISA. Constituents, which may include anyone or any entity in the public, use forms located on the website to complete these activities. Incident reports are primarily submitted using CISA's internet reporting system,