- HSIN Optimization and Development Vision
  - Improving System Performance and Service Operations—A summary of the steps the program has and will be taking to ensure the current platform meets user service requirements and agreements.
  - Interoperability and Federation—A discussion of the program's plans to link HSIN to a series of partner networks that will provide all users with greater access to new collaborative partners and their content.
  - Large List—A summary of how the program is implementing new ways to ensure the validation of users is fast and efficient.
  - New Development Environments—A discussion on how HSIN is creating a set of new virtual environments for its new development team to use that are stable and accurately replicate the actual network, to ensure, final, new developments work as planned and meet requirements.
  - DHS Suspicious Activity Reporting (SAR)—An introduction to how HSIN is developing a new capability for the quick and efficient delivery and sharing of suspicious activity reports by users of all kinds including those from the private sector.
- Portal Consolidation Update—A review of HSIN's efforts to save resources across the Federal government by consolidating a series of systems into the single, HSIN platform.
- Public comment period
- Deliberation/Voting/Obtain guidance from HSINAC on:
  - Stakeholder Management Strategy—A review of HSIN's new strategy for ensuring managed growth, user self-sufficiency, and prioritized engagements with critical partners in the coming year.
  - Messaging/Communications Strategy—An update on HSIN's work to define its place in the information sharing market, what defines it, its value proposition, and the best way to communicate these terms.
  - HSIN Mobile Use/Application Policy—An opportunity for HSINAC members to comment on the development of a new policy that will define the rights, duties and privileges to use HSIN on mobile devices ensuring security and accessibility.
- Closing remarks
- Adjournment of the meeting

James Lanoue,

HSIN Acting Program Manager.

[FR Doc. 2013–28703 Filed 11–27–13; 8:45 am]

BILLING CODE 9910–9B–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2013–0078]

Cooperative Research and Development Agreement (CRADA) Opportunity With the Department of Homeland Security for the Testing of Reusable Electronic Conveyance Security Device (RECONS) Solutions

AGENCY: Borders and Maritime Security Division (BMD), Homeland Advanced Research Projects Agency, Science and Technology Directorate, Department of Homeland Security.

ACTION: Notice of intent.

SUMMARY: BMD is initiating a project to demonstrate that commercially available conveyance security solutions can be utilized with a common data management system in the following Government operations (described in detail later):

- Centralized Examination Station (CES)
- In-bond
- National Capital Region Secure Delivery
- Cross-border Commerce

BMD is looking to enter into a Cooperative Research and Development Agreement (CRADA) with interested partner(s) to test the interoperability and conveyance security capabilities of their solutions in a lab environment and then assess their ability to support CES, In-bond, National Capital Region Secure Delivery, and Cross-border Commerce operations in a technology demonstration.

The results of the project are intended to serve as a data point for the standard under development for reusable electronic conveyance security devices (RECONS). The RECONS Standard will support certification of partner solutions to be used by industry for their cross-border commerce shipments (described in detail later) in addition to the Government in their aforementioned operations.

The proposed term of the CRADA can be up to twenty-four (24) months.

DATES: Submit comments on or before December 30, 2013.

ADDRESSES: Mail comments and requests to participate to Jonathan McEntee, (ATTN: Jonathan McEntee, 245 Murray Lane SW., Washington, DC 20528–0075). Submit electronic comments and other data with the subject line ''RECONS Notice of Intent'' to *jonathan.mcentee@dhs.gov.*

FOR FURTHER INFORMATION CONTACT:

Information on DHS CRADAs: Marlene Owens, (202) 254–6671.

SUPPLEMENTARY INFORMATION:

Background

Ensuring cargo security as it flows through supply chains is a challenge faced by industry and governments, both domestically and internationally. There is a need to identify illegal activity introduced into the supply chain while facilitating the flow of legal commerce.

A solution that provides greater security and facilitation of legal commerce is tracking the cargo conveyance as it moves through the supply chain and reporting any security breaches. The additional data is critical in assessing the risk level of cargo shipments and determining which shipments require more scrutiny rather than expedited processing.

Operational Context

Each operation requiring conveyance security is slightly different and it is important to understand the environment in which they will be employed to ensure understanding of the unique characteristics.

Centralized Examination Stations (CES) Operations: Ports of entry (POEs) often are constrained in the physical space and resources available to conduct physical inspections at the facility. In order to prevent arriving conveyances awaiting inspection from negatively impacting the flow of shipments through the POEs, shipments selected for physical inspection are often directed to a facility (i.e. CES) located away from the POE. The shipments are secured with high security International Organization Standard (ISO) bolts while they are en route between the two facilities and legally remain within custody of CBP until they are cleared at the CES.

Using RECONS in CES Operations will increase security by providing tracking between the POE and CES and ensuring they do not deviate from the designated route and/or compromise the integrity of the conveyance and the shipment. In addition, using RECONS for repeated trips rather than single-use ISO bolts will automate processes resulting in cost savings and efficiencies in operations.

In-bond Operations: Duties are nominally assessed when a shipment

arrives at a POE and is then cleared to enter into U.S. commerce. Some shipments pass through the U.S. while in transit to another country and never enter the U.S. commerce. Additional shipments are allowed to travel within the U.S. and defer their payment of duties until they are entered into U.S. commerce at their formal port of entry. These shipments (in-bond shipments) are required to post a bond which CBP can collect against to insure the shipments do not enter U.S. commerce without paying the requisite duties. CBP secures some of these shipments with ISO bolts when they initially arrive at a U.S. POE and verifies the integrity of the ISO bolt when the shipment either exits the U.S. via a POE or enters U.S. commerce.

Using RECONS in In-bond Operations will allow for the collection of data that can be used to determine if any cargo was illegally off-loaded into U.S. commerce resulting in collecting against the insurance bond as well as serving as a deterrent to illegal activity. In addition, RECONS will automate processes leading to efficiencies while also saving money over time than employing single-use ISO bolts.

National Capital Region (NCR) Secure Delivery: Trucks making deliveries to buildings managed by GSA within the National Capital Region are first screened at a central facility and then secured with mechanical seals before delivering the cargo.

Using RECONS in NCR Secure Delivery Operations will increase security by providing tracking between the FPS scanning facility and the delivery and ensuring they do not deviate from the designated route to introduce illegal or dangerous cargo. The tracking data also verifies delayed deliveries and the reasons cited for arriving outside of the designated window thus avoiding the need for them to return to the FPS scanning facility to be re-inspected. In addition, RECONS will automate processes leading to efficiencies and cost savings.

Cross-border Commerce: Conveyance security extends beyond just CES, In-bond, and National Capital Region Secure Delivery within the Government, with other agencies such as DOE and DOD requiring conveyance security solutions.

There is a much larger need for conveyance security solutions for commercial cross-border commerce with over *$1 trillion* of goods being imported every year. Currently the only approved solutions are ISO bolts although there are much better solutions already in the commercial market. The impediment to adopting these enhanced solutions is they are not certified for use and the root cause of that is there is no standard to certify conveyance security solutions against.

The development of a RECONS Standard will be conducted by BMD in parallel with this project along with efforts to update CBP systems and policies to accept and use the data provided by RECONS for cross-border shipment processing. A spiral approach is being pursued with additional capabilities added to the RECONS Standard and CBP systems, supported by updated CBP policies, as the use of RECONS in cross-border operations evolves.

Period of Performance

If CRADA collaborator(s) is (are) selected, laboratory testing is expected to take 2 months. Contingent on laboratory testing, operational testing is expected to take an additional 6 months and data consolidation, analysis, and results finalization is expected to take another 3 months.

Selection Criteria

The Borders and Maritime Security Division (BMD) reserves the right to select CRADA collaborators for all, some, or none of the proposals in response to this notice. BMD will provide no funding for reimbursement of proposal development costs. Proposals (or any other material) submitted in response to this notice will not be returned. Proposals submitted are expected to be unclassified.

BMD will select proposals at its sole discretion on the basis of:

1. How well the proposal communicates the collaborators' understanding of and ability to meet the CRADAs goals and proposed timeline.

2. Ability of the collaborator to provide equipment and materials for proposed testing.

This includes the ability of the collaborator to provide a sufficient number of RECONS for laboratory and operational testing within two months of CRADA agreement.

3. Ability of the collaborator to invest in system and RECONS development costs to ensure interoperability with government system.

4. How well the proposal addresses the following criteria:

a. Ability of the collaborator to meet the requirements for development ,[1] validation testing and analysis, and submission of supporting data and documents fulfilling the RECONS laboratory and operational testing.

b. Ability of the collaborator to provide RECONS that are hardened to prevent tampering and have had environmental testing performed consistent with the operational conditions the RECONS will be employed.

c. Ability of the collaborator to provide documentation of the entire system required to operate RECONS and the all the associated costs throughout the lifecycle for procuring, operating, and maintaining RECONS.

d. Ability of the collaborator to provide RECONS that provide intrusion detection and tracking along with secure data exchanges, while maintaining a low false alarm and failure rate.

Participation in this CRADA does not imply the future purchase of any materials, equipment, or services from the collaborating entities, and non-Federal CRADA participants will not be excluded from any future BMD procurements based solely on their participation in this CRADA.

Authority: CRADAs are authorized by the Federal Technology Transfer Act of 1986, as amended and codified by 15 U.S.C. 3710a. DHS, as an executive agency under 5 U.S.C. 105, is a Federal agency for the purposes of 15 U.S.C. 3710a and may enter into a CRADA. DHS delegated the authority to conduct CRADAs to the Science and Technology Directorate and its laboratories.

Dated: November 21, 2013.

Stephen Hancock,

Acting Director, Office of Public-Private Partnerships.

[FR Doc. 2013–28531 Filed 11–27–13; 8:45 am]

BILLING CODE 9110–9F–P

[1] Development work may be needed to ensure solutions meet interoperability or other requirements validated through testing

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket No. USCG–2013–0522]

Tank Vessel Oil Transfers

AGENCY: Coast Guard, DHS.

ACTION: Notice; reopening of comment period

SUMMARY: The Coast Guard issued a notice in the **Federal Register** of October 23, 2013, concerning new measures to reduce the risks of oil spills in oil transfer operations from or to a tank vessel. In response to public comments requesting an extension of the original comment period ending on November 22, 2013, the Coast Guard is reopening the comment period for an additional 30 days.