

## 1. GENERAL INFORMATION

**Agency Name:** Department of Homeland Security  
Science & Technology Directorate  
Washington, DC 20528

**Research Opportunity Title:** DHS S&T Long Range Broad Agency Announcement

**Research Opportunity Number:** BAA 14-02

**Catalog of Federal Domestic Assistance (CFDA) Number:** 97.065

**Catalog of Federal Domestic Assistance (CFDA) Title:** Homeland Security Advanced Research Projects Agency

**Response Date:** This is a five (5) year announcement and will remain open until December 31, 2018, 11:59PM, Eastern Standard Time (EST). White Papers are due by this response date; thus, if you are encouraged to submit a Full Proposal based on your White Paper submission, please be advised that the due date of the full proposal will be the date that is specified in the notification letter; and not the response date by December 31, 2018, 11:59PM, EST.

However, if an offeror's proposal is not encouraged based on their White Paper submission, and the offeror still opts to submit a full proposal, they may do so within 60 days of the notification letter; and not the response date by December 31, 2018, 11:59PM, EST.

### Points of Contact:

Sally Harris  
LRBAA Coordinator  
Department of Homeland Security  
Science & Technology Directorate  
245 Murray Lane, SW  
Mail Stop 2100  
Washington, DC 20528-2100  
[LRBAA.Admin@hq.dhs.gov](mailto:LRBAA.Admin@hq.dhs.gov)

Jenista M. Featherstone  
Contracting Officer  
Department of Homeland Security  
Office of Procurement Operations  
245 Murray Lane, SW  
Mail Stop 0115  
Washington, DC 20528-3051  
[s&t-2014-lrbaa@hq.dhs.gov](mailto:s&t-2014-lrbaa@hq.dhs.gov)

S&T BAA Website: <https://baa2.st.dhs.gov>

S&T BAA Website Tech Support: [dhsbaa@reisis.com](mailto:dhsbaa@reisis.com) or (703) 480-7676

## 2. INTRODUCTION

The Department of Homeland Security (DHS) Science & Technology Directorate (S&T) reserves the right to reject submissions if the work proposed duplicates current S&T activities, falls outside the particular division's current efforts, or does not comply with the submission instructions. Therefore all interested parties must read these instructions carefully.

This is a Long Range Broad Agency Announcement (LRBAA), as contemplated in Federal Acquisition Regulation (FAR) 6.102(d)(2) and 35.016. It is not a request for information (RFI). The LRBAA's submission and evaluation processes are distinct from those of conventional procurements that use Requests for Proposals (RFPs) or Requests for Quotes (RFQs).

S&T's mission is to "support basic and applied homeland security research to promote revolutionary changes in technologies; advance the development, testing and evaluation, and deployment of critical homeland security technologies; and accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities." This Announcement declares S&T's general interest in competitively funding R&D projects across a spectrum of science and engineering disciplines. S&T will focus on areas where risk inhibits mission or operational investments, and where significantly improved or increased capability payoffs can be expected.

S&T seeks R&D projects for revolutionary, evolving, and maturing technologies that demonstrate the potential for significant improvement in homeland security missions and operations. The unique contribution of your proposed research or technical concept, and how it differs from similar efforts or solutions, must be clearly articulated in your White Paper. Offerors should read the descriptions of the research topic areas of interest and identify the specific topic for which their concept will have the maximum impact. Offerors are encouraged to select the one division that most directly corresponds to their proposed subject matter.

It cannot be emphasized too strongly that all submissions must indicate significant advancement in the evolution of a topic area identified in this Announcement. The Government reserves the right to reject submissions that do not clearly articulate such advances or innovations.

This announcement is restricted to work relating to basic and applied research and that portion of advanced technology development *not* related to a specific system or hardware procurement. This announcement does *not* cover support services, such as technical services, engineering services, or other types of support services to include "contracting"-type services (e.g., quasi-directed subcontracting) or contracts to "evaluate" another contractor's performance/program. Such submissions are considered non-compliant with this LRBAA and will be rejected without evaluation.

Fully developed products are not normally considered under this LRBAA, unless the Offeror is proposing a totally different application for the product or a modification is needed, which requires substantial research. Purchase of capital equipment will only be allowed under a given

proposal if S&T deems it reasonable and necessary to conduct the particular project. No LRBA award shall be primarily for the purchase of capital equipment.

Offerors who seek, through this LRBA, to extend work previously completed must clearly articulate where the old work ended, where the new work begins, and what new advances are expected from the work contemplated under this LRBA. Please ensure it is clear that the work now being submitted is independent of previous work (i.e. the next logical step in the research, or investigating a subject that was discovered and not funded under the previous award). Submitting existing Statements of Work and indicating which steps have been completed is not sufficient justification for an independent award under the LRBA.

DHS S&T will not issue paper copies of this Broad Agency Announcement. Oral presentations are not permitted at any point during the LRBA process.

### **3. ELIGIBILITY INFORMATION**

All responsible Offerors are eligible to submit White Papers under the LRBA, but DHS S&T particularly encourages submissions from small businesses. However, no set aside of any kind will be made.

Foreign or foreign-owned Offerors are advised that their participation is subject to foreign disclosure review procedures, applicable export control laws, and other applicable federal laws, regulations, and policies pertaining to U.S. Government business with foreign entities.

Offerors may include independent organizations, single entities, or teams from private sector organizations, Government laboratories, airport authorities, Federally Funded Research and Development Centers (FFRDCs), and academic institutions. FFRDCs, including the Department of Energy National Laboratories and Centers, are eligible to respond to this LRBA individually or as team members with eligible principal Offerors, as long as they are permitted to respond to such announcements under their applicable sponsoring agreements.

Historically Black Colleges and Universities (HBCUs), Minority Institutions (MIs), small businesses, small disadvantaged businesses, women-owned small businesses, service-disabled veteran owned small businesses, and HUBZone small businesses are encouraged to submit proposals and to join other entities as team members in submitting proposals.

Offerors must be prepared to cooperate and exchange data and technical information as requested by DHS S&T. Data rights and intellectual property terms and conditions will be addressed after Full Proposal evaluation.

The cost of preparing White Papers and Full Proposals in response to this Announcement is not considered an allowable direct cost. Offerors should consult FAR 31.205-18 when considering whether these costs may be allocated as indirect costs. The Contracting Officer will determine allowability and allocability. The Offeror may be required to submit certified cost and pricing data if the value of a prospective award exceeds the Truth in Negotiations Act threshold.

#### **4. AWARD INFORMATION**

The S&T technical subject matter expert personnel shall coordinate with the Contracting Officer to identify White Papers that present “particular value” to S&T. The Division Contracting Officer will encourage the Offerors of these White Papers to submit Full Proposals consisting of detailed technical and cost information. Please note that any such encouragement does not assure an award.

The primary basis for selecting proposals for acceptance shall be technical, importance to agency programs, and funding availability. Cost realism and reasonableness shall also be considered to the extent appropriate. Therefore, DHS S&T reserves the right to select for negotiation of a potential award to fund all, some, or none of the Full Proposals received in response to this Announcement. The amount of resources made available under this BAA will depend on the quality of the proposals received and the availability of funds. A proposal may be selected, but only specific portions may be of interest. The award value and period of performance of each selected Full Proposal will be determined on a case-by-case basis.

Proposal development costs will not be reimbursed. Technical and cost proposals (or any other material) submitted in response to this BAA will not be returned. However, depending on the markings on the proposal, DHS S&T will adhere to FAR policy on handling source selection information and proprietary proposals. It is the policy of DHS S&T to treat all proposals as proprietary information and to disclose their contents only for the purposes of evaluation.

Multiple awards are anticipated through this LRBA. Award decisions will be based on a competitive selection of proposals resulting from a scientific and cost review. Awards *may* take the form of Time-and-Materials/Labor Hour or Cost-Reimbursement type contracts. However the Government also reserves the right to award grants, cooperative agreements, Other Transaction Agreements (OTA) (if authorized by law at time of award), or interagency agreements to appropriate parties should the situation warrant.

The applicable laws and regulations governing a particular award will depend on that award vehicle. S&T will also facilitate access to laboratory and operationally relevant test and evaluation facilities, where reasonably available. In the event that an Offeror or subcontractor is an FFRDC, Department of Energy National Laboratory, or other federal entity, DHS S&T will work with the appropriate sponsoring agency to issue an interagency agreement pursuant to the Economy Act (31 USC 1531) or other appropriate authority.

In many cases, other elements of the U.S. Government are pursuing related technologies. In such cases, S&T will leverage those technology development efforts wherever it is practicable and efficient to do so.

#### **5. ETHICAL CONSIDERATIONS**

*Communication During Evaluation:* Once a White Paper or Full Proposal has been submitted, the evaluation becomes active until the LRBA Contracting Officer issues an official notification letter to the Offeror. During the evaluation (White Paper or Full Proposal), **no**

**communication shall occur** between S&T personnel and the Offeror regarding the submission or its general subject matter, except as noted below.

During the evaluation period, the LRBA Contracting Officer must be the focal point of any exchange with Offerors. After receipt of a Full Proposal, no discussion regarding the scope of work, resources required to execute the scope, etc., will be allowed during the Source Selection process. However, a Contracting Officer may initiate communications if and when specific facts in the submission require further clarification from the Offeror (such as confirmation of a delivery date).

*Conflict of Interest:* Per HSAR 3025.209-72, *Organizational Conflict of Interest* issues will be evaluated on a case-by-case basis as outlined below:

- (a) Disclosure. In a Full Proposal submission Offerors must represent to the best of their knowledge: (1) whether any of their current employees were previously employed by DHS S&T, and whether any of their former employees are now DHS S&T employees; (2) full disclosure of any actual, potential, or perceived organizational conflicts of interest. The Offeror shall include a mitigation plan for any actual or potential conflicts of interest, in accordance with paragraph (d) of this provision.
- (b) Determination. The Contracting Officer may determine that this effort may result in an actual, potential, or perceived conflict of interest.
- (c) If an Offeror with an actual, potential, or perceived conflict of interest believes it can be mitigated the Offeror may submit a mitigation plan to the Contracting Officer. The Contracting Officer may approve a mitigation plan; reject a mitigation plan and ask for revisions; or reject a mitigation plan, determine that the conflict of interest cannot be resolved or avoided, and find the Offeror ineligible for award.
- (d) Other Relevant Information. In addition to the mitigation plan, the Contracting Officer may require additional relevant information from the Offeror. The Contracting Officer will use all information submitted by the Offeror, and any other relevant information known to DHS, to determine whether an award may be made and whether the mitigation plan adequately mitigates the conflict.
- (e) Corporation Change. The successful Offeror shall inform the Contracting Officer, within 30 calendar days of the effective date of any corporate mergers, acquisitions, or divestitures that may affect this provision.
- (f) Flow-down. The contractor shall insert the substance of this clause, paragraphs (a) through (f), in each subcontract that exceeds the simplified acquisition threshold.

Offerors who have existing contract(s) with DHS S&T for scientific, engineering, technical or administrative support will receive particular scrutiny.

Note also that FAR-based awards will incorporate Homeland Security Acquisition Regulation (HSAR) clause (deviation) 3052.209-70 Prohibition on Contracts with Corporate Expatriates.

## 6. PRE-SUBMISSION INQUIRIES

A pre-submission inquiry is optional. The LRBAAs webpage has a submission portal specifically for pre-submission inquiries. Through this portal only, you may submit a brief statement of your idea and receive general feedback on if the idea meets the mission of DHS. Inquiries emailed directly to divisions will not be considered. S&T personnel can indicate whether an idea appears to be within the scope of the division's interests and this LRBAAs. S&T personnel cannot assist in the preparation of a White Paper, nor can they propose any ideas they would like Offerors to address. However, regardless of the feedback you receive, you may still submit a White Paper.

Go to <https://baa2.st.dhs.gov> and click on the following links: (1) Current Solicitations; (2) LRBAAs 14-02; (3) Pre-Submission Inquiry. This will take you to the online pre-submission inquiry portal. You will be asked to identify a topic area to ensure it is routed to the correct division and individual(s).

## 7. RESEARCH TOPICS

Below are brief treatments of the topic areas of interest. In your White Paper submission, you will be asked to identify the division and/or specific topic area that best fits your proposed research.

### **BORDER AND MARITIME SECURITY**

The Borders and Maritime Security division is interested in the development and evaluation of security technologies and pilot testing new surveillance, tracking, and response capabilities that cover vast expanses of remote border territories. Our focus is on technologies that improve the security of our Nation's borders and waterways without impeding the flow of commerce and travelers.

Border and Maritime Security's overarching goals are as follows:

Goal 1: Develop advanced detection, classification, and locating technologies that will enhance law enforcement officers' ability to secure the border and respond to border threats.

Goal 2: Develop advanced detection, identification, interdiction, and enforcement technologies for rapid, coordinated response to maritime threats.

#### **BMD.01 Land Border Security**

- Detection of, tracking of, classifying of, and responding to all threats along the terrestrial and maritime border – specifically, technologies that can perform one of the following functions:
  - Noninvasive, minimally disruptive sensors and systems that can detect and locate clandestine, unknown subterranean threats (tunnels and other buried objects of interest to law enforcement) within varied geologies of the southwest border.

- Cost-effective airborne sensors for better land border security to assist in locating illicit activities, materials, or their means of conveyances, including:
  - Runway-agnostic unmanned aerial systems that could be evaluated on their ability to provide ground operators with situational awareness and airborne imagery of areas of interest
  - Unmanned systems development and demonstration for detecting, responding to, characterization or classification of threats to include illicit border crossings, drug trafficking, severe weather, and natural disasters; and
  - Persistent wide area ground and aerial surveillance capabilities for long duration monitoring of border areas

## **BMD.02 Maritime Border Security**

The technologies and concepts described under Maritime Border Security will be evaluated under the concepts that define the DHS S&T Coastal Surveillance System (CSS) Project for FY 14 through FY 2018. The CSS project fields a new enterprise-grade information sharing system, new information sources, and new information analytics for DHS and other federal, state, territorial, tribal, and local partners. The project seeks to expand and enhance CSS by adding new data sources/capabilities to detect/track maritime vessels. Promising capabilities defined in the following categories will be required to demonstrate suitability of use including ease of connectivity and operational effectiveness. The categories are:

- Improved systems – enhancements to the common operating picture and intelligence capabilities to incorporate new capabilities and provide better cross-domain support;
- Improved situational awareness by tracking small boat activity, detecting anomalous and/or illegal behavior, and providing timely and actionable information in support of law enforcement and port security efforts.
- Improved sensor performance to enable improved detection and tracking of small and large vessels by overcoming environmental clutter issues within the port/harbor as well as in coastal environments as well as improved dissemination of radar, video, and other information;
- Concepts, methodologies, and/or technologies that utilize public as well as private databases, data sets, data collection devices, or sensors of opportunity to increase detection/tracking accuracy and/or the field of regard surrounding inland waterways, ports, harbors, and coastal regions.

The CSS employs open standards and necessary information will be provided to selected technologies/capabilities/concepts at no cost to facilitate connectivity to the CSS enterprise architecture and will undergo an interoperability assessment. Interoperability assessments are planned to occur at a minimum of two activities each year at various venues and selected technologies will be invited to participate. Participation at these events will not be limited to capabilities that are selected via this LRBA process. Other avenues will also be pursued to discover and evaluate technologies for potential connection to the CSS enterprise and interoperability assessments.

## **CYBER SECURITY DIVISION**

The Cyber Security Division focuses on research for advanced cyber security and information assurance solutions to secure the Nation's current and future cyber and critical infrastructures against persistent threats and dynamic attacks. This research is guided by the President's National Strategy to Secure Cyberspace and Comprehensive National Cyber Security Initiative. These solutions include secure protocols, end system security, user identity and data privacy technologies, research infrastructure, law enforcement forensic capabilities, competitions, and education.

**CSD.01** – Internet Infrastructure Security – including secure internet protocols including Domain Name System Security (DNSSEC) and Secure Protocols for Routing Infrastructure (RPKI and BGPSEC).

**CSD.02** – National Research Infrastructure – mimicking real-life conditions, systems and infrastructure, to enable the cyber security research community to discover, test, and analyze state-of-the-art tools, technologies and software in a scientifically rigorous and ethical manner.

**CSD.03** – Homeland Open Security Technology – Open Source Security Technology to enable implementation and deployment of open source security technologies in Federal, State, and Local environments.

**CSD.04** – Forensics support to law enforcement – including the research and development of tools and technologies that will allow investigators to visualize, analyze, share and present data derived from cell phones, GPS devices, computer hard drives, networks, and other digital media.

**CSD.05** – Identity Management (IdM) - seeking tools, technologies, credential vulnerability studies, and other efforts that improve the security of access control in both cyber and physical environments. The mission of the IdM research projects is to develop, test, and evaluate interoperable tools, technologies, standards, and protocols for the purpose of controlling user access within and outside of organizational boundaries. The foundational goal is to increase security and productivity while decreasing cost and security risks.

**CSD.06** – Data Privacy Technologies - seeking to develop a set of technologies and associated business processes, which help organizations responsibly manage personally identifiable information (PII) in a manner that protects individual privacy consistent with applicable law, policy, and mission. Data Privacy tools that inherently provide privacy are critical enablers of information sharing as they automate control of privacy data and foster confidence that personal information is being used appropriately while minimizing privacy risk. Data Privacy projects support the application of technologies to the transfer, management, and accountability of privacy data for federal, state, local, and critical infrastructure and key resource information sharing missions by exploring, refining and integrating technologies and techniques, and piloting the results.

**CSD.07** – Software Assurance – The CSD objective in the area of Software Assurance is to develop and improve Software Analysis technologies, tools, and techniques to reduce the exposures and vulnerabilities in software. The nation's critical infrastructure (energy, transportation, telecommunications, banking and finance, and others), businesses, and services

are extensively and increasingly controlled and enabled by software. Vulnerabilities in software put the nation's critical resources at risk. To address this objective, CSD is seeking research in areas such as:

- a) Software analysis techniques for vetting untrustworthy software to address Software Supply Chain Risk Management. Specifically, analysis capabilities for – malicious code detection, covert channel detection, denial of service susceptibility, and Botnet/Malware detection. Software definitions as defined by Common Weakness Enumeration (CWE) should be used for categorization.
- b) Vulnerability correlation engine to reduce false-positives and improve detection capabilities for false-negatives. This may include combining run-time analysis, dynamic tracing, fuzzing, static analysis, and other types of code inspection techniques to improve coverage in programming languages, as well as weakness classes.
- c) Tool modernization to improve techniques, methods, and services in static analysis to advance state-of-the-art. Technologies to leverage code quality techniques to improve static analysis workflows, such as code refactoring.
- d) Secure coding techniques to assist developers with software development activities to improve coding practices, serve as an education and awareness component for developers in avoiding problematic and egregious software coding errors.
- e) Threat and attack model simulations to cover areas such as business logic flaws, system environment, OS related exposures.
- f) Mobile code assessments – support Android and iOS mobile applications. The discovery and detection of applicable CWEs for mobile code issues.
- g) Smart and intelligent Integrated Development Environment (IDE) that integrates static analysis workflows to improve program correctness, program structure (reusability, encapsulation), and code restructuring.

**CSD.08** – The CSD objective in the area of cyber security education is to develop, demonstrate and help implement comprehensive and dynamic cyber security education models that impact our homeland and national cyber security education condition for the better. These models and associated technologies need to support cyber security competitions and education and curriculum development. To address this objective, CSD anticipates cyber security research in areas such as:

- a) the coupling of operations with education and training;
- b) abstract learning versus learning with context;
- c) Bayesian learning (prior knowledge) and where and how it might be applicable.

**CSD.09** – Cyber-physical control and Critical Infrastructure Systems and Security – The intersections of cyber security and critical infrastructure is a growing vulnerability for the American homeland, characterized by tight coupling, coordination, and interconnections among sensing, communications, computational, control, information and physical resources. Their interconnections in particular form a complex system of systems, and the complexity of these systems and interconnections will continue to grow. The complexity of systems poses challenges in resiliency, vulnerability, threat, and recovery assessment. To address this area, CSD is interested in applied research addressing areas such as:

Models, theories, methods, and tools to fully address the cyber security of cyber-physical systems, in a unified and integrated way;

Analysis, understanding and control approaches at the intersection of security analysis and operations analysis, i.e. possible overlaps between control and critical infrastructure systems and their cyber security, industrial security and operations security capabilities;

The interplay of control, business and consumer-facing systems, and the interplay between different critical infrastructure systems;

Security architectures, in particular how different security approaches might best work to protect critical infrastructure systems.

**CSD.10** – Internet Measurement and Attack Modeling Techniques: Security focused measurement and attack modeling for all aspects of cyberspace. This includes the Internet (e.g., ASNs, routers) as well as other devices (e.g. medical devices) or networks (e.g. ICS) that may connect to the Internet, via a static or dynamic (possibly intermittent) connection. Security focused measurement includes but is not limited to algorithms, tools, techniques, data and analysis for enabling security, from global scale to the individual user. Attack modeling includes not only models of various attacks, but models of how to secure a system from attacks, either internal or external, at scales that may include individuals, enterprises, or the entire Internet. There is also interest in models of attacks on systems that intermittently connect the Internet and how to secure such systems. The security focus of models is broadly interpreted, to include such topics as attack attribution, secure composition of systems, and other related topics.

**CSD.11** – Securing the mobile workforce: Technologies to support flexible client-side security, including secure protocols to protect data flow to, within and out of the cloud; data integrity; user privacy constraints; forensics analysis to preserve digital evidence; and measurement systems to identify unauthorized activity.

**CSD.12** – Insider Threat - research in the areas of understanding and identifying threats and potential risks, development of trustworthy systems with specific policies to hinder insider misuse, and remediation when insider misuse is detected but not prevented.

**CSD.13** – Experiments and Pilots – Technologies developed through federally funded research requiring test and evaluation in experimental operational environments to facilitate transition.

**CSD.14** –Research Data Repository – Cyber security datasets of interest to the research community.

**CSD.15** – Cyber Security Economic Incentives – Research into the areas of: Cybersecurity insurance and cyber behaviors (individual and organizational)

- a) Economic, policy, and regulatory interactions in the promulgation and implementation of cybersecurity measures
- b) Testing and demonstrating the utility of cyber economic incentives
- c) Business models for cybersecurity investment and for cybercrime – the boundary between incentives and disincentives
- d) Applications of modern game theory to cybersecurity

**CSD.16** – Data Analytics – The exponential increase in the volume of data created daily worldwide creates new challenges for cyber security. S&T is interested in technologies and tools to support the analysis of datasets whose size is beyond the ability of commonly used software tools to capture, manage and process. These include but are not limited to:

- a) Data discovery,
- b) automated analysis techniques,
- c) machine and self-learning algorithms and
- d) data visualization.

**CSD.17** – Tailored Trustworthy Spaces – Technologies and tools supporting the concepts of tailored trustworthy spaces, including but not limited to:

- a) trust negotiation tools and data trust models to support negotiation of policy,
- b) Type-safe languages and application verification, and tools for establishment of identity or authentication as specified by the policy, and
- c) Support for application-aware anonymity to allow for anonymous web access, and platform security mechanisms and trust-in-platform.

**CSD.18** - Distributed Denial of Service Defense – Denial of service attacks are pervasive and have the potential to disrupt critical network infrastructure. Topics of interest include:

- a) efforts that leverage existing policies and practices to mitigate DDoS attacks,
- b) techniques that adopt existing technologies for near term DDoS protection, and
- c) novel approaches for measuring and understanding DDoS attacks and new techniques for future DDoS mitigation.

## **EXPLOSIVES COUNTERMEASURES DIVISION**

Explosives Countermeasures include the detection, mitigation, and response to explosive threats including: all modes of transportation within the Transportation Systems Sector (Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline); in checked and carry- on baggage; Home Made Explosives (HME); improvised explosive devices (IEDs), vehicle borne (VBIED) and person borne (PBIED); and response and defeat technologies.

**EXD.01** – Standoff Detection of Explosives: Technologies for the standoff detection of explosives and explosive devices related to Person and Vehicle Borne Improvised Explosive Devices. Explosives of interest include commercially available explosives (i.e. Ammonium Nitrate based), conventional military explosives (i.e. Composition C-4 and Semtex A/H) and homemade explosives (i.e., peroxide base). Standoff Detection implies that both the detection equipment and operator be located at some distance (>1 m up to tens of meters) away from the subject or object under interrogation. Subtopics include:

- (1) Integration of both multimodal and multispectral technologies for improved detection and/or imaging metrics.
- (2) Development of automated detection and/or identification capabilities associated with both imaging and spectroscopy based technologies.

**EXD.02** – Trace Detection of Explosives: Technologies for the detection of explosives trace particle and vapor signatures in aviation security, facilities protection, and mass transit security operations. Specific interests include handheld and benchtop explosives trace detection (ETD) systems, optical methods for quickly and quantitatively measuring trace contamination on a range of surfaces, and advanced explosives trace detection system concepts.

**EXD.03** – Cargo Security includes detecting intrusion or unauthorized access, positively identify cargo, and provide timely response – in particular, in containerized, palletized, parcel, or bulk/break-bulk maritime, air cargo, and freight rail.

**EXD.04** – Test and Evaluation Expertise and Facilities for Counter-IED detection technologies. Standoff, Remote, and Checkpoint based explosives detection systems, to be evaluated, most often require real explosives and local storage of said explosives. Facilities must be able to store, on-site, small amounts (< 1 pound) of various solid explosives, while achieving clean, uncontaminated facilities for equipment testing. Facilities must be able to accommodate non-eye safe laser ranges, x-ray based screening equipment, and neutron-based screening equipment. Facilities must also be able to accommodate, in certain cases, large, outdoor vehicle borne IED screening equipment.

**EXD.05** – Data Fusion and Automated Detection for aviation cargo, checked baggage, carry-on baggage, personal check points and all surface intermodal concerns. Algorithms and techniques for detection fusion and automated alerting that combines a variety of detection modalities, including but not limited to X-ray, trace chemical detection, computed tomography (CT) and video.

**EXD.06** – Advanced Detection Technologies: Development of robust, enhanced explosives detection methods such as fluorescence quenching materials, bio-inspired molecular recognition techniques and advanced sampling technologies to improve selectivity and sensitivity capabilities. Detection methods should be easily deployed, low cost and require minimum training to operate. Special attention should be paid to determining better sensing mechanisms and signal amplification mechanisms to apply to future detection improvements. Advanced image processing and data collection methods are of interest.

## **FIRST RESPONDER GROUP**

The First Responder Group identifies, validates, and facilitates the fulfillment of First Responder capability gaps through the use of existing and emerging technologies, knowledge products, and the acceleration of standards. The FRG focuses on: (1) developing tools, technologies, methodologies, standards, protocols, and guidance to enable improved communications interoperability for First Responders; (2) providing First Responder solutions for high-priority capability gaps through rapid prototyping; (3) maintaining a Web portal that enables First Responders to easily access and leverage Federal web services; and (4) overseeing the National Urban Security Technology Laboratory, which provides a test and evaluation capability for DHS-developed technologies and systems.

**FRG.01** – The ability to identify trends, patterns, and important content from large volumes of information from multiple sources (including non-traditional sources) to support incident decision-making. Improvements in this Capability can: (1) Prevent incident command and general staff from being overloaded with unmanageable amounts of incident data; (2) Allow incident commanders to synthesize and analyze information to make informed operational decisions. Capability Requirements: (1) Tools to analyze incoming incident data in real-time to identify trends, patterns and anomalies; (2) Policies and standards to utilize such information to inform and improve decision making.

**FRG.02** – The ability to share video from incident scene to medical services personnel in a remote location. Improvements in this Capability can: (1) Gather EMS color requirements for compressed video; (2) result in improved compression for video streaming in order to transmit it over the limited available wireless bandwidth. Capability Requirements: (1) applications must retain color truth throughout the video system.

**FRG.03** – The ability to analyze the performance of a video system’s transport component. Improvements in this Capability can: (1) use different types of cameras (e.g., high definition, low definition) to identify the limits of camera use for streaming video (with or without compression) on a given network; (2) help define network bandwidth requirements for a video applications. Capability Requirements: (1) efficient use of bandwidth for a specific video application on a user’s given device.

**FRG.04** – The ability to better understand how the public will respond to alert and warning messages on mobile devices. Improvements in this Capability can: (1) Improve understanding of the public’s response to alerts and warnings, including how to optimize message content, message frequency, education and training, communicating to special populations, message diffusion throughout the public, and trust and validation of messages; (2) Take into consideration current Commercial Mobile Alert Service (CMAS) regulations proposed by the CMSAAC and supported by the FCC, including enhanced geo-targeting features; (3) Understand the use of social media and public participation in origination and dissemination of alerts and warnings including research and testing in the areas of standardization, aggregation and analysis, behavioral response, best practices, and privacy. Capability Requirements: (1) Consideration of current CMAS regulations as proposed by the CMSAAC and supported by the FCC.

**FRG.05** – The ability to better determine when more granular geo-targeting (i.e. below the County level as currently implemented) is appropriate as well as how broadly targeting should be extended from the point of incident. Improvements in this Capability can: (1) Accelerate geo-targeting standardization; (2) Enable the creation and establishment of best practices and standard operating procedures for adoption; (3) Focus on areas such as addressing messages across boundaries between targeted regions, differing coverage areas across multiple mobile carrier networks, the challenges of in-building geographies such as airports, and other enhancements to improve the geo-targeting of mobile alerts and warnings using cell broadcast. Capability Requirements: (1) Geo Targeting (i.e., below the County level as currently implemented).

**FRG.06** – The ability of local responders to respond to and recovery from a radiological/nuclear incident. Improvements in this capability can: (1) Assist local responders in managing the complexity of the response; (2) Allow for complete characterization of the incident, including hazard identification; (3) Provide capability to protect citizens, families, and responders in the initial response; (4) Provide initial medical care for survivors; (5) Provide long-term care for incident casualties and evacuees; (6) Allow for stabilization and control of the impacted area and infrastructure; and (7) Manage long term radiological clean-up and restoration of essential functions.

**FRG.07** – The ability to monitor airborne radioactive fallout particles that have been released into the atmosphere, identifies the fallout composition/half-life, and accurately track its path and dispersion. Improvements in this Capability can: (1) Provide real-time information for decision makers responsibly for ordering evacuations and protective actions; (2) Allow for a rapid response coordination by identifying safe areas for resource staging and operations; (3) Provide citizens information about how to best protect themselves and their family; Capability Requirements (1) tracking information must be available for access by local decision makers (2) information must have the ability update in a reasonable timeframe to influence decisions being made.

## **RESILIENT SYSTEMS DIVISION**

RSD's mission is to develop and deploy S&T solutions that enable the Homeland Security Enterprise and community of users to enhance preparedness, mitigate hazards, ensure effective response, execute rapid recovery, minimize risks to critical infrastructure and impact on the societal resilience and economy, and enable free flow of commerce in order to improve national resilience. RSD currently focuses on three portfolios of R&D: human factors/identification systems, physical security systems, and decision support systems. An important objective of RSD is to ensure that R&D solutions yield products that will be deployed into operational environments for the user communities.

### **Human Factors/Identification Systems**

This portfolio applies the social and behavioral sciences to improve detection, analysis, and understanding of threats posed by individuals, groups, and radical movements; develops novel technologies and tools to improve the recognition of individuals; supports the preparedness,

response, and recovery of communities impacted by catastrophic events including support for first responders; and advances national security by integrating human factors and public perceptions data into homeland security technologies. The identification aspects of this portfolio focus on biometric solutions that are agile, fail proof, and cost effective. The areas of interest in this portfolio are:

**RSD 1.1** – Behavior-based methods, models, trainings and technologies to enhance community resilience in the face of human- or nature-caused catastrophes through such means as better understanding of risk perception; improved risk communication by emergency responders and public officials; pre-event education and training; and applied theoretical and empirical research into the properties of resilient social networks and communities to include elements of social media and crowd sourcing..

**RSD 1.2** – Research and development to improve the detection, analysis, understanding, and mitigation of the threats posed by violent extremists. Knowledge, tools and technologies to determine when individuals, groups, and movements are likely to engage in violence, and what ideological, organizational, and contextual factors may influence violent action.

**RSD 1.3** – Methods for non-invasively identifying deceptive and suspicious behavior within a time constrained, low-base rate, screening environment, and methods for identifying interactive strategies optimal for eliciting disguise-resistant indicators of deceptive and suspicious behavior, including technologies that automate or aid in such identification. Protocols and technologies to minimize insider threats and to identify insider threat behavior when it occurs, especially in settings like transportation security or at a border are of interest as well.

**RSD 1.4** – Improvements in biometrics, including real-time positive verification of individual identity using multiple biometrics; mobile biometrics screening capabilities, high-fidelity ten print capture, non-cooperative biometric technologies for identification and the development of standards and test/evaluation protocols.

## **Physical Security Systems**

This portfolio focuses on innovative and effective solutions to reduce damage from natural hazards, minimize their impact on critical infrastructure, and provide the ability to quickly recover from disasters. Examples of hazards include hurricanes and the heat engine processes that control their intensity and resulting storm surge; solar storms resulting in geomagnetic impacts on earth; flooding and erosion, and flooding; wildfires; and processes driven by high winds and drought, including protective design and rapidly deployable protective measures; and earthquakes, including an ability to interpret signals from the earth to estimate the timing, location, and severity of an earthquake. The areas of interest in this portfolio are:

**RSD 2.1** – Surveillance Systems are of interest including video analytics, fusion algorithms, and intelligent filtering algorithms to identify, recognize, and track potential threatening events, behaviors, and individuals in a high density operational environment such as an aviation- or ground-based mass transit portal. These systems can also provide early detection and warning of earthquake, wild fire and other natural hazards to disaster management agencies, the general

population and critical infrastructure owners/operators. Integrating multiple types of sensing technologies and intelligent algorithms and processing data will allow for more efficient acquisition and interpretation of data and move complex systems towards more efficient enterprise deployments.

**RSD 2.2** – Resilient and Sustainable Infrastructure: Enhance security, resilience, and recovery of the 18 critical infrastructure sectors for retrofit applications. Develop key critical infrastructure components that can easily transition to user application, are affordable (in acquisition as well as operations and maintenance), highly transportable, and offer robust solutions for use during manmade and natural disruptions. Integrate infrastructure protection design with sustainable technologies and methodologies; reducing the consumption of energy, promote clean water, decrease pollutant emissions, and aiming to conserve resources over the life of the component. Key critical infrastructure component design should consider use of high-performance green materials that are self-monitoring, self-healing should stand the test of time; and should resist blast, earthquake, floods, and wind. Developing infrastructure that is sustainable means thinking differently about how we build, what we build, and whether we build at all. It means designing and maintaining infrastructures that are both highly efficient and all-hazard-resistant. Additionally, this portfolio addresses solutions that offer innovative risk/threat/consequence analysis processes, and methodologies to support the evaluation of national resilience against all hazard events.

### **Decision Support Systems**

This portfolio focuses on systems that will enable the nation to enhance resilience to all hazard events through collection and integration of data/information, analysis of risk and consequences, and dissemination of actionable results in a timely manner. The areas of interest in this portfolio are:

**RSD 3.1** – Agile Decision Aid Analytics to include mathematical methods, computational algorithms, and software/hardware architectures for discovering, comprehending, fusing and manipulating diverse, disparate data or information and applying the resulting knowledge to assess threats and consequences, anticipate terrorist incidents and natural or manmade catastrophic events, and guide response and recovery activities. Analytical capabilities that can operate on relatively small data sets to provide useable just-in-time response strategies (logistics, resource requirements) to improve resilience are of interest.

**RSD 3.2** – Modeling, Simulation, and Gaming technologies: Concepts, techniques, methodologies, algorithms, and innovative tools and applications to significantly enhance the quality of system analysis and reduce the time/cost of conducting system analyses. Develop modeling tools for a wide range of decision makers, from local law enforcement to governors to the White House, to evaluate alternative policies and actions to deal with emergencies and anticipate cascading effects across interdependent systems. Tools for real-time decision support in emergencies capable of integrating and assimilating multiple types of information, processing that information, and presenting it in a manner useful to decision makers. Capabilities sought include the following: Simulation Based Exercise, Training, Education in both real time and non-real time Dynamic, on-Demand, and Real-time Information Processing and Visualization; Innovative model integration technologies and standards Simulation Based Response Doctrine,

Policy/Guidance Analysis, Exercise, and Training; Mobile, Light-weight, and portable device integration into Modeling and Simulation Environments

**RSD 3.3** – Geospatial and Remote Sensing: Geospatial technologies enhancing situational awareness for the disaster management and protection of critical infrastructure resulting in improved incident management at the Federal, State, and local and tribal levels. Develop image processing and spatial analytical techniques that exploit remote sensing measurements resulting in improving the detection of specific phenomena of interest to public safety and first responders. Using analytics and automation software that will allow for data integration, develop mathematical methods, computational algorithms, and hardware architectures for discovering, comprehending, and manipulating diverse, diffuse data or information and applying the resulting knowledge to develop baseline assessments, assess threats and consequences, anticipate terrorist incidents and natural or manmade catastrophic events, and guide response and recovery activities. Integrate capability into web services that improves analytical capability using cloud computing or distributive architectures to provide critical products to all levels of incident command.

**RSD 3.4** – Emergency Management: Advances to improve protection of or enhance performance of emergency responders as they carry out life-saving tasks. Develop technologies that will fully enable emergency managers and responders to effectively cope with multi-hazard emergencies— technologies such as integrated advanced materials for protective clothing that report on the health of the first responder; decision support systems that provide real-time logistical tracking and management of emergency supplies, equipment, and personnel; advanced precision indoor/outdoor tracking technologies; integrated simulation-based incident planning and response capability to analyze all-hazard disaster response and recovery operations, tactics, techniques, plans, and procedures for use in a real-time environment for simulation-based training; advanced algorithms, tools, and infrastructures for sensor data fusion and visualization for improved situational awareness and emergency response to include wireless communications, both in secure and quasi-secure environments.

**RSD 3.5** – Information Sharing: Supports improved situational awareness and decision making across Federal, state, local, tribal and territorial public safety organizations, as well as non-governmental agencies, private sector partners organizations and the public and communities. Seeks concepts, prototypes and technologies that improve the capability to collect, process, analyze, visualize, share, and protect information across the Homeland Security Enterprise.

## **8. SUBMISSION PROCESS AND CLASSIFIED INFORMATION**

All LRBAAs submissions must be made through the S&T BAA website at <https://baa2.st.dhs.gov>. Select *Proposal Submission* from the side menu, then *Register*. You will need to know your company's Tax Identification Number to complete the registration. Submissions will not be accepted from unregistered organizations. Once registered, log into the system and select BAA 14-02. Contact technical support for the website at [dhsbaa@reisys.com](mailto:dhsbaa@reisys.com) or (703) 480-7676.

*Oral presentations are not permitted at any point during the LRBA process. A White Paper submission is mandatory. Full Proposals will be rejected outright if they are not preceded by a White Paper. The Offeror must receive an official notification letter from the Contracting Officer regarding the White Paper's evaluation results prior to submitting the corresponding Full Proposal.*

There is no limit to the number of different White Papers a particular Offeror may submit; however, if a White Paper is not encouraged, do not resubmit the same one or a slightly modified version of it. If an Offeror feels that a White Paper fits multiple topics, select the one topic that best fits the proposed research.

In teaming situations, the lead organization must remain the same on both the White Paper and, if selected, the Full Proposal. Any Full Proposal submitted by an entity other than the prime at the time of the White Paper submission will be rejected.

Submissions will be protected from unauthorized disclosure in accordance with FAR 15.207, applicable law, and DHS regulations. Offerors are expected to mark appropriately each page of their submissions that contains proprietary information.

## **Classified Information**

**Only unclassified** pre-submission inquiries, White Papers, or Full Proposals may be submitted via the LRBA website. **Classified information must not be transmitted via the LRBA website.** Instructions for submitting classified information are provided below.

The Government encourages contractors to work at the unclassified level whenever possible. In situations where a project consists of classified and unclassified elements, the information shall be segregated and marked appropriately. If a project or deliverable consists of classified and unclassified elements that cannot be segregated, the contractor shall use methods and conventions appropriate for classified environments.

The contractor may be required to have access to, and may be required to receive, generate or store classified information. Any contractor facilities used would require appropriate facility clearances and have the capability to store classified material. A DD Form 254 is required prior to accessing or producing any classified information. Additionally, the contractor is required to safeguard the information labeled as proprietary. Any security concerns must be addressed to Shane Davis, Science and Technology Directorate, Department of Homeland Security; unclassified email: shane.davis@hq.dhs.gov; classified email: [shane.davis@dhs.gov](mailto:shane.davis@dhs.gov); office: 202-254-5749.

Offerors of classified information must first register online and submit to the website a placeholder PDF file consisting of a single page with the words "Classified Volume Forthcoming" in the center of the page. Then print out the completed cover sheet for your placeholder submission, and attach it to the classified submittal. The classified submittal must be submitted via proper classified courier or proper classified mailing procedures as described in the National Industrial Security Program Operating Manual (NISPOM). The NISPOM document is

online at [http://www.dss.mil/isp/fac\\_clear/download\\_nispom.html](http://www.dss.mil/isp/fac_clear/download_nispom.html). Classified submittals must include ten (10) printed copies and one electronic copy on compact disc recordable (CD-R) media (do not use re-writable media, e.g. CD-RW/RW-/RW+). Each copy must be accompanied by the coversheet, which does not count towards the page limitations.

The email address for *classified* submissions is [shane.davis@dhs.gov](mailto:shane.davis@dhs.gov). Also, send an *unclassified* email alert to [shane.davis@hq.dhs.gov](mailto:shane.davis@hq.dhs.gov) and [s&t-2014-lrbaa@hq.dhs.gov](mailto:s&t-2014-lrbaa@hq.dhs.gov) **before** emailing classified information to [shane.davis@hq.dhs.gov](mailto:shane.davis@hq.dhs.gov).

## 9. CONTENT AND FORMAT

### White Papers

- ✓ White Papers shall be no more than five (5) pages long. Offerors shall use the White Paper format included as Appendix 1 of this document. No exceptions.
- ✓ Paper Size – 8.5 x 11 inch paper
- ✓ Margins – 1 inch
- ✓ Spacing – single or double-spaced
- ✓ Font – Times New Roman, 12 point
- ✓ Convert the original document into a PDF (portable data format) file. Useful information regarding file conversions may be accessed online at the U.S. Grants website: [http://grants.gov/help/download\\_software.jsp](http://grants.gov/help/download_software.jsp).
- ✓ The submission portal will automatically generate a cover page with your identifying information.

### Full Proposals

- ✓ Full Proposals consist of two volumes: Technical (vol.1) and Cost (vol.2)
- ✓ Paper Size – 8.5 x 11 inch paper
- ✓ Margins – 1 inch
- ✓ Spacing – single or double-spaced
- ✓ Font – Times New Roman, 12 point
- ✓ Number of Pages: **The Technical Proposal is limited to no more than 40 single-sided pages.** The Cost Proposal has no page limitations; however, it shall only contain information necessary for determination of cost appropriateness. All technical information must be presented in the Technical Proposal only. The cover page, table of contents, resumes, and list the of intellectual property as cited at Append 2 are excluded from the page limitations. The Subcontracting Plan, if applicable, is included in the page limitation. *See description of a cover page and cover sheet below.*
- ✓ Excel files are not permitted and must be converted to a PDF file to be uploaded to the LRBA submission portal.
- ✓ Files shall not exceed 10 megabytes in size. A Full Proposal shall consist of two (2) electronic files in PDF format.

## Full Proposal Content

### Volume 1: Technical Proposal

Volume 1 of the Full Proposal must include the following sections:

- Cover Sheet is automatically generated during the submission of the White Paper to the LRBA website. *This is not the same as the Offeror's cover page.*
- Cover Page shall include the words "Technical Proposal" and the following:
  - 1) BAA number 14-02;
  - 2) Title of proposal;
  - 3) Topical area and its reference code;
  - 4) Identity of the prime Offeror, including name and address, and complete list of subcontractors, including name and address, if applicable;
  - 5) Technical contact (name, address, phone, electronic mail address);
  - 6) Administrative/business contact (name, address, phone, electronic mail address);
  - 7) Duration of effort (separately identify the basic effort and any options);
  - 8) DHS S&T point of contact, if applicable;
  - 9) Dunn & Bradstreet (DUNS) number;
  - 10) Acknowledgement that the Offeror is registered in Central Contractor registration (CCR). This can be established at the System for Award Management (SAM) website at <https://www.sam.gov/portal/public/SAM/>;
  - 11) Statement specifying compliance with FAR Clause 52.222-54 "Employment Eligibility Verification."
  - 12) Confirmation of U.S. Citizenship for those participating in the project, and the identity of any proposed personnel or subcontractors who are not U.S. citizens.
- Official Transmittal Letter with authorizing official signature. For an electronic submission, the letter can be scanned and incorporated into the electronic proposal. The letter of transmittal shall state whether this proposal has been submitted to another government agency other than DHS S&T and, if so, which one and when.
- Table of Contents
- Executive Summary of the proposed research and benefits expected from this investment.
- Landscape Assessment or Brief Literature Review: Explain why your proposal is different and superior to similar solutions already available or to the efforts of others who have been researching similar issues.
- Proposed Use for DHS S&T: A detailed explanation of how the proposed product(s) supports the targeted end user (e.g., the first responder community) in an operational context. Include quantitative specifications for how the products will improve operational performance.

- Technical Concept: A description of the technical concept, including anticipated risks and approaches to mitigate the risks. Describe the basic scientific or technical concepts that will be used in each component or subsystem comprising your proposed solution to the problem described above. What particular scientific, technical or engineering issues need to be addressed and resolved to demonstrate feasibility? What is unique about your solution and what advantages might it afford compared to alternative approaches that others have taken? What has been the extent of the principal investigator's past experience in, and qualifications or educational background for, developing the technologies in your proposal?
- Operational Concept: A description of the operational concept used in the proposed technical solution to accomplish the objectives. Explain how the performance of your proposed solution can be expected to meet or exceed and be measured against each of the specific technical attributes and/or performance enhancements. What are the key scientific, technical, or engineering challenges and the timing for each that must be met in order to successfully complete this project? Describe all required material and information, which must be provided by the Government to support the proposed work.
- Operational Utility Assessment Plan : A detailed plan for demonstrating and evaluating the operational effectiveness of the Offeror's products in exercises, including evaluation metrics. Explain your view of the requirements gap to be filled, what capability will be provided upon successful completion of the proposed effort, and what are the technical risks associated with successful maturation of the proposed effort to achieve operational utility. Explain your concept of how you will develop and demonstrate a system or system component. Identify and explain the critical path technologies or key technical challenges you will face when building this system or component and your plans for meeting these challenges. Explain how you will demonstrate the system or component performance relative to the performance or enhancement goals described in the proposal.
- Statement of Work: A Statement of Work (SOW) and a Work Breakdown Structure (WBS) that clearly detail the scope and objectives of the effort, the technical approach, and the performance goals. The SOW and WBS will be used in the development of any final award, so the proposal must include a stand-alone SOW and a stand-alone WBS without any proprietary restrictions. The WBS must include a detailed listing of the technical tasks/subtasks in hierarchical fashion for the tasks required to accomplish the effort. The WBS format must be complete to at least WBS level three. Each task in the SOW shall describe the work to be carried out, the end result of the task, the time allocated, the organization performing the task, the predecessor tasks, the performance goals of the task, and the resources (labor, materials, and services) required. The resources shall be costed to provide a baseline budgeted cost for the applicable task. The SOW shall be at a level sufficient to define the nature of the work to be carried out, measure progress, and demonstrate the relationship of the tasks to one another.
- Project Schedule and Milestones: A summary of the schedule of events and milestones. If applicable, identify the critical path.

- Deliverables: A detailed list and description of all deliverables and data deliverables the Offeror proposes to provide to the Government, the schedule for delivery, and acceptance criteria. The deliverables information must be a separate section in the Offeror's proposal and begin on a new page. Proposals must include a severable self-standing detailed list and description of all deliverables without any proprietary restrictions, which can be used to make award.
- Qualifications: A discussion of the Offeror's previous accomplishments and work in this area, or closely related area, and the qualifications of the investigators. If the proposal involves development or testing scientific and/or engineering concepts, the principal investigators must demonstrate education and/or managerial expertise in these fields. Key personnel resumes must be attached to the proposal and do not count toward the page limitations.
- Detailed Risk Mitigation Plan: Discuss in detail the technical, cost, and schedule risk(s) involved with the project and how each risk will be mitigated.
- Management Approach: A discussion of the overall approach to the management of the effort, including brief discussions of the total organization, use of personnel, project, function, and subcontractor relationships, government research interfaces, and planning, scheduling and control practice. Identify which personnel and subcontractors (if any) will be involved. Include a description of the facilities that are required for the proposed effort with a description of any Government-Furnished Equipment/Hardware/ Software/ Information required, by version and/or configuration.
- Small Business Considerations: Full Proposals that exceed \$650,000, submitted by all but small business concerns, must include a Small Business Subcontracting Plan in accordance with FAR 52.219-9. The Small Business Subcontracting Plan is included in the 40 page limit. Regardless of the proposed dollar value, all Offerors shall indicate their business size status and list all subcontractors and their business size statuses. All LRBA Offerors are encouraged to offer subcontracting opportunities to small businesses to the maximum extent practicable.
- Employment Eligibility Verification: Include a statement specifying compliance with FAR Clause 52.222-54.
- Intellectual Property: In accordance with FAR 52.227-15, Representation of Limited Rights Data and Restricted computer Software (Dec 2007)

(a) This solicitation sets forth the Government's known delivery requirements for data (as defined in the clause at [52.227-14](#), Rights in Data—General). Any resulting contract may also provide the Government the option to order additional data under the Additional Data Requirements clause at [52.227-16](#), if included in the contract. Any data delivered under the resulting contract will be subject to the Rights in Data—General clause at [52.227-14](#) included in this contract. Under the latter clause, a Contractor may withhold from delivery data that qualify as limited rights data or restricted computer software, and deliver form, fit, and function data

instead. The latter clause also may be used with its Alternates II and/or III to obtain delivery of limited rights data or restricted computer software, marked with limited rights or restricted rights notices, as appropriate. In addition, use of Alternate V with this latter clause provides the Government the right to inspect such data at the Contractor's facility.

(b) By completing the remainder of this paragraph, the offeror represents that it has reviewed the requirements for the delivery of technical data or computer software and states [*offeror check appropriate block*]—

[ ] (1) None of the data proposed for fulfilling the data delivery requirements qualifies as limited rights data or restricted computer software; or

[ ] (2) Data proposed for fulfilling the data delivery requirements qualify as limited rights data or restricted computer software and are identified as follows: **See below.**

---

(c) Any identification of limited rights data or restricted computer software in the offeror's response is not determinative of the status of the data should a contract be awarded to the offeror. (End of provision)

Offerors responding to this BAA must submit a separate list of all technical data or computer software according to the template provided at Appendix 2 that will be furnished to the Government with other than unlimited rights. The Government will assume unlimited rights if offerors fail to identify any intellectual property restrictions in their proposals. Include in this section all proprietary claims to results, prototypes, and/or deliverables. If no restrictions are intended, then the offeror should state "NONE."

## Volume 2: Cost Proposal

- Cover Sheet: The cover sheet is automatically generated during the submission of the White Paper to the LRBA website. *This is not the same as the Offeror's cover page.*
- The cost proposal must consist of a cover page and two parts. Part 1 is a detailed breakdown of all costs by cost category by calendar and Government fiscal year. Part 2 further breaks down this information as it pertains to each task or sub-task.
- The following information must be provided for the base year and any proposed option(s) or option year(s):
  1. Part 1 must provide a detailed cost breakdown of all costs by cost category by calendar and Government fiscal year. (Provide a time-phased spend plan).
  2. Part 2 must provide a detailed cost breakdown by task/sub-task using the same task numbers in the Statement of Work. (Provide Basis of Estimates – contractor format is permitted.)
  3. Identify any cost drivers.
  4. Options must be separately priced.
- Cover Page: The use of the SF 1411 is optional. The words "Cost Proposal" must appear on the cover page in addition to the following information:
  1. BAA Number 14-02;
  2. Title of proposal;

3. Topical area and reference code;
4. Identity of prime Offeror, including name and address, and complete list of subcontractors, including names and addresses, if applicable;
5. Technical contact (name, address, phone/fax, electronic mail address);
6. Administrative/business contact (name, address, phone/fax, electronic mail address);
7. Duration of effort (separately price out the basic effort and any options);
8. DUNS number and CAGE code;
9. Statement on whether or not the Offeror has been audited by a Government organization (Defense Contract Audit Agency, Office of Naval Research, etc.), and if the Offeror has a Government-approved accounting system;
10. DCAA point of contact (name, telephone number, and email address);

### **Cost Proposal Part 1**

Part 1 of the cost proposal must include a detailed breakdown of all costs by cost category by calendar and Government fiscal year and include a summary explaining how each element is applied in the cost proposal:

- Direct Labor: Individual labor category or person, with associated labor hours and **unburdened** direct labor rates.
- Indirect Costs: Fringe Benefits, Overhead, G&A, COM, etc. (Must show base amount and rate).
- (If applicable and available) Forward Pricing Rate Agreement (FPRA) or Defense Contract Audit Agency (DCAA) approved or recommended rates. Identify if there are outstanding CAS violations. Offerors please note the following:

In order to qualify for the award of a cost reimbursement contract, the offeror must have an adequate accounting system in accordance with FAR 16.301-3(a)(1). Evidence of an adequate accounting system would include a written opinion or other statement from the cognizant federal auditor (CFA) or the cognizant federal agency official (CFAO) that the system is approved or has been determined to be adequate. If available, the offeror shall provide the audit report number and date associated with the accounting system review. If the offeror does not have a copy of the report, the offeror may furnish a copy of the audit report number.

If the offeror does not have an accounting system that has been determined adequate by the CFA or CFAO, but believes its accounting system is adequate, the offeror shall so state in its proposal. As part of the pre-award evaluation process, the Government will obtain the necessary review by the CFA. The offeror will be required to allow the CFA to review the accounting system and correct (or have a timely action plan to correct) any issues identified as precluding the system from being adequate. The offeror will provide the CFA name, address and telephone number and the point of contact as part of its proposal.

Offers will be rejected if the offeror does not have an adequate accounting system unless the Government determines that the offeror's action plan for correcting the accounting system is timely and acceptable. However, no costs will be paid under the contract until the Contractor's system has been determined adequate.

**FOR TIME-AND-MATERIALS/LABOR HOUR –**

In order to qualify for the award of a time-and-material/labor hour contract, the offeror must have an adequate accounting system in accordance with FAR 16.301-3(a)(1). Evidence of an adequate accounting system would include a written opinion or other statement from the cognizant federal auditor (CFA) or the cognizant federal agency official (CFAO) that the system is approved or has been determined to be adequate. If available, the offeror shall provide the audit report number and date associated with the accounting system review. If the offeror does not have a copy of the report, the offeror may furnish a copy of the audit report number.

If the offeror does not have an accounting system that has been determined adequate by the CFA or CFAO, but believes its accounting system is adequate, the offeror shall so state in its proposal. As part of the pre-award evaluation process, the Government will obtain the necessary review by the CFA. The offeror will be required to allow the CFA to review the accounting system and correct (or have a timely action plan to correct) any issues identified as precluding the system from being adequate. The offeror will provide the CFA name, address and telephone number and the point of contact as part of its proposal.

Offers will be rejected if the offeror does not have an adequate accounting system unless the Government determines that the offeror's action plan for correcting the accounting system is timely and acceptable. However, no invoices will be paid under the contract until the Contractor's system has been determined adequate.

The Contractor shall maintain an adequate accounting system to substantiate vouchers (including any subcontractor hours reimbursed at the hourly rate in the schedule) by evidence of actual payment and by:

- (i) Individual daily job timekeeping records;
  - (ii) Records that verify the employees meet the qualifications for the labor categories specified in the contract; and
  - (iii) Other substantiation approved by the Contracting Officer. (FAR 52.232-7(a)(5)).
- Travel: Separate by destinations and include number of trips, durations in number of days, number of travelers, per diem (travel costs, hotel and meals in accordance with the Federal Travel Regulations and FAR PART 31), airfare, car rental, if additional miscellaneous expense is included, list description and estimated amount, etc.
  - Subcontracts: Subcontractors must each submit a cost proposal that is as detailed as the Offeror's cost proposal. The subcontractor's cost proposal can be provided securely in

electronic submission with the Offeror's cost proposal, or will be requested from the subcontractor at a later date. The subcontractor's cost proposal must be on company letterhead and include the complete company name and mailing address, technical and administrative/business point of contacts, email address, and telephone number. Include the DUNS number. The prime Offeror must submit a copy of its subcontracting agreement(s). The Contracting Officer may elect to waive this requirement.

- Consultants: Provide consultant agreement or other documents which verify the proposed loaded daily/hourly rate and labor category.
- Materials: Materials amounts must be specifically itemized with costs or estimated costs. Where possible, indicate purchasing method (e.g., competition, engineering estimate, market survey, etc.). Include supporting documentation, i.e. vendor quotes, catalog price lists, and past invoices for similar purchases.
- Other Directs Costs: Other Direct Costs (ODCs), particularly including any proposed equipment or facilities. Equipment and facilities generally must be furnished by the Offeror. Justifications must be provided when Government funding for such items is sought.
- Fee/Profit: Must including fee percentage or, if calculated differently, amount.
- Spend Plan: Provide a time-phased spend plan which includes all costs proposed, i.e., labor, travel, materials, and ODCs (contractor format is acceptable).
- Basis of Estimate: Provide a basis of estimate (BOE) for all proposed labor. The BOE must provide the rationale for the proposed labor category(ies) and proposed labor hours for each labor category (contractor format is acceptable).

## **Cost Proposal Part 2**

Cost breakdown by task/sub-task using the same task numbers in the Statement of Work.

## **10. SIGNIFICANT DATES**

This announcement will remain open until 11:59PM, Eastern Standard Time on December 31, 2018. White Papers are due by this response date. If your White Paper is of interest, and you are encouraged to submit a Full Proposal, then the due date for your Full Proposal will be specified in your White Paper notification letter. This new due date, set by the Contracting Officer for your Full Proposal submission, supersedes the date on which this BAA expires.

Offerors who are not encouraged to submit a Full Proposal may nevertheless submit one within 60 days of receiving the White Paper notification letter.

Evaluations and awards will occur on a "rolling selection" basis. Generally, evaluations should occur within 60 days from receipt of the White Paper, and 120 days for a Full Proposal. This is not a firm commitment to 60 or 120 days, but every effort will be made to conduct reviews as expeditiously as possible.

Awards resulting from a selected Full Proposal are projected to occur within approximately 90 days after award notification (i.e. approximately 180 days after submission), contingent upon successful negotiations with the DHS Contracting Officer and/or subject to availability of funds. Full Proposals submitted should cite a validity timeframe of 180 days.

## **11. PROPRIETARY PROTECTION**

Submissions will be considered proprietary information and will be protected accordingly as long as they are appropriately marked. DHS S&T has contracted for business and staff support services, including assistance with LRBAAs submissions (reference below **NOTE**). Contractors will provide administrative support. Submissions will be evaluated only by authorized Government employees; only Government employees will sit on Source Selection Evaluation Boards. In submitting a White Paper or Full Proposal, Offerors consent to allow contractor access to submissions. All contractors who provide support services to S&T for LRBAAs activities have signed general non-disclosure agreements and, where applicable, organizational conflict of interest statements.

**NOTE:** The Government may obtain support from both Federal SMEs and support contractor when completing LRBAAs evaluations. Support contractors may be used to provide administrative assistance to federal employees who are involved in the evaluation of white papers and full proposals. Administrative assistance would include tracking the white papers/full proposals through the review process and assigning white papers and full proposals by system assigned number or white paper/full proposal title. Contractors will have limited system access which does not include the capability to read or review white papers or full proposals. As the activities typically carried out under the LRBAAs do not involve advisory and assistance services (A&AS) contractors *evaluating or analyzing* proposals, the limitation in FAR 37.203(d) will not apply. If the conflict described in FAR 9.505-4 is found to exist, S&T will ensure that the contractors conclude the necessary agreements, which are kept on file, before proprietary information is shared.

## **12. EVALUATION INFORMATION**

Due to the large number of submissions received, DHS S&T is unable to offer technical feedback to Offerors for White Papers. Offerors who receive notification that S&T has discouraged further interest in a White Paper may still proceed with the submission of a Full Proposal. Upon request and within a three (3) business day receipt of the notification letter the DHS S&T will provide Offerors with technical feedback on all Full Proposals resulting from encouraged White Papers, regardless of whether an award is ultimately made based on the Full Proposal. DHS S&T personnel will provide this feedback as quickly as possible after examining the Full Proposals, but due to the large volume of submissions Offerors are encouraged to be patient. DHS S&T will also attempt to provide feedback on Full Proposals resulting from discouraged White Papers, but Full Proposals resulting from encouraged White Papers will be more highly prioritized.

## **Evaluation Factors and Subfactors**

### **White Papers**

White Papers will be evaluated according to the following factors and subfactors. The subfactors are specified under each factor. (Factors are indicated alphabetically, and subfactors are indicated numerically. Not all factors have subfactors.)

*Evaluation factors A and B listed below are of equal importance, and more important than factors C. Each subfactor under its factor is of equal weight within the factor; not all factors have subfactors.*

#### **A. Overall scientific and technical merits of the proposal.**

1. The degree of innovation and potential to offer a revolutionary increase in capability or a significant reduction in cost commensurate with the potential risks of the innovative approach;
2. The soundness of the technical concept;
3. The Offeror's awareness of the state-of-the-art and future technology trends;
4. The Offeror's understanding of the scope of the problem and the technical effort needed to address it;
5. Intellectual Property rights offer;
6. The Offeror's understanding of the project's risks, and how these risks have been identified and how they are being addressed; and
7. How the proposed solution compares to similar work performed.

#### **B. Mission relevance.**

Extent to which the work proposed applies to the topic area (as described beginning on page 6) to which the White Paper was submitted and the needs of S&T.

#### **C. The Offeror's capabilities, related experience, and past performance, including the qualifications, capabilities, and experience of the proposed principal investigator and personnel.**

1. The quality of technical personnel proposed and/or proposed key personnel;
2. The Offeror's experience in relevant efforts with similar resources;
3. The Offeror's ability to manage the proposed effort;
4. Provide a list of similar contracts, delivery orders, purchase orders, and/or subcontracts (hereafter referred to as "contracts") completed during the past 3 years, a list of similar contracts currently in process, or a combination of both. Similar contracts listed may include any contract entered into with the federal Government, agencies of state and local governments, and commercial customers. Offerors that are newly formed entities without prior similar contracts shall associate proposed personnel with similar current or completed contracts. Include the following information for each contract, and list of similar grants/cooperative agreements, if unclassified and possible to disclose:

- Name of contracting activity;
- Contract number;
- Contract type;
- Total contract value;
- Description of contract work;
- Contracting Officer name, telephone number, and email address;
- COTR name, telephone number, and email address (if applicable);
- Administrative Contracting Officer's name, telephone number, and email address (if different from the Contracting Officer listed above);
- List of first-tier subcontractors.

### **Full Proposals**

Full Proposals will be evaluated according to the following factors and subfactors. The subfactors are specified under each factor. (Factors are indicated alphabetically, and subfactors are indicated numerically. Not all factors have subfactors.)

*Evaluation factors A and B listed below are of equal importance, and more important than factors C, D, and E. Factors C, D, and E are listed in descending order of importance. Each subfactor under its factor is of equal weight within the factor; not all factors have subfactors.*

A. Overall scientific and technical merits of the proposal.

1. The degree of innovation and potential to offer a revolutionary increase in capability or a significant reduction in cost commensurate with the potential risks of the innovative approach;
2. The soundness of the technical concept;
3. The Offeror's awareness of the state-of-the-art and future technology trends;
4. The Offeror's understanding of the scope of the problem and the technical effort needed to address it;
5. Intellectual property rights offered
6. The Offeror's understanding of the project's risks, and how these risks have been identified and addressed; and
7. How the proposed solution compares to similar work performed.

B. Mission relevance.

1. Extent to which the work proposed applies to the topic area (as described beginning on page 6) to which the proposal was submitted and the needs of S&T.

C. The Offeror's capabilities, related experience, and past performance, including the qualifications, capabilities, and experience of the proposed principal investigator and personnel.

1. The quality of technical personnel proposed and/or proposed key personnel;
2. The Offeror's experience in relevant efforts with similar resources;

3. The Offeror's ability to manage the proposed effort;
4. Provide a list of similar contracts, grants/cooperative agreements, delivery orders, purchase orders, and/or subcontracts (hereafter referred to as "contracts") completed during the past 3 years, a list of similar contracts currently in process, or a combination of both. Similar contracts listed may include any contract entered into with the federal Government, agencies of state and local governments, and commercial customers. Offerors that are newly formed entities without prior similar contracts shall associate proposed personnel with similar current or completed contracts. Include the following information for each contract, if unclassified and possible to disclose:
  - Name of contracting activity;
  - Contract number;
  - Contract type;
  - Total contract value;
  - Description of contract work;
  - Contracting Officer name, telephone number, and email address;
  - COTR name, telephone number, and email address (if applicable);
  - Administrative Contracting Officer's name, telephone number, and email address (if different from the Contracting Officer listed above);
  - List of first-tier subcontractors.

D. Cost/Price, including cost reasonableness.

Each response will be reviewed for cost reasonableness and the particular value it offers to the Government. Members of the evaluation team may presume that the Offeror's technical approach serves as a rationale for the labor mix and labor hours used.

E. Extent of subcontracting commitment.

For proposed awards to be made as contracts to large businesses, the small business consideration section of each proposal will be evaluated based on the extent of the Offeror's commitment to providing meaningful subcontracting opportunities for small businesses, small disadvantaged businesses, woman-owned small businesses, HUBZone small businesses, veteran-owned small businesses, service disabled veteran-owned small businesses, historically black colleges and universities, and minority institutions. All Offerors shall indicate their business size status (listed above) and list each subcontractor and its business size status. Full Proposals that exceed \$650,000, submitted by all but small business concerns, must include a Small Business Subcontracting Plan in accordance with FAR 52.219-9.

Full proposals will be selected for possible award based on a competitive selection of proposals resulting from a scientific and cost review.

## 13. AWARD ADMINISTRATION INFORMATION

### Administrative Requirements

- **NAICS:** The North American Industry Classification System (NAICS) code for this announcement is 541712 with a small business size standard of 500 employees.
- **CCR:** Successful Offerors not already registered in the Central Contractor Registry (CCR) will be required to register in CCR prior to award of any grant, contract, cooperative agreement, or other transaction agreement. Information regarding CCR registration is available at the System for Award Management (SAM) website at <https://www.sam.gov/portal/public/SAM/>.
- **Certifications:** In accordance to FAR Part 4.11, all prospective contractors shall be registered in the System for Award Management (SAM) prior to award. The SAM is the official U.S. government system that consolidates the capabilities of CCR/FedReg, ORCA and EPLS. There is NO fee to register for SAM. If you used any of the previous systems, you should now go to [www.sam.gov](http://www.sam.gov) to update your information. SAM training tools and quick-start guides are available on both the SAM and Federal Service Desk websites, located at [www.sam.gov](http://www.sam.gov) and [www.fsd.gov](http://www.fsd.gov).
- **Subcontracting Plans:** Full Proposals that exceed \$650,000, submitted by all but small business concerns, must include a Small Business Subcontracting Plan in accordance with FAR 52.219-9. The Small Business Subcontracting Plan is included in the 40 page limit.
- **Federal Travel Regulations (FTR):** Information on per diem rates based on travel locations are provided on [www.gsa.gov](http://www.gsa.gov). Also, refer to FAR PART 31 for information on travel costs.

### Reporting

The following are samples of data deliverables that are typically required under a research effort:

- Technical and financial progress reports;
- Test results, data, and analyses;
- Presentation materials (includes pictures);
- Other documents or reports;
- Report of demonstration;
- Monthly program report;
- Final technical report.

The following minimum deliverables will be required under traditional procurement contracts awarded to those Offerors whose Full Proposals are selected for award:

#### Monthly Program Report

Brief (not more than two pages) narrative reports must be submitted to the program manager in accordance with the terms of the contract

#### Final Technical Report

For a final report, each selected Offeror must provide a technical report of work performed during the period of performance, delivered no later than the last day of the period of

performance. The final report must be a cumulative, stand-alone document that describes the work of the entire test and evaluation period leading up to it. It must detail how the design prototype was refined or otherwise prepared for the test and evaluation program and, if applicable, why such refinements or preparations were undertaken. It must include any technical data gathered, such as measurements taken, models developed, simulation results, and formulations developed. The final report must include a summary of all performance goals versus performance achieved during the program (either measured or otherwise substantiated). The final report must discuss all variances from the performance goals versus performance achieved, including reasons or theories for variances. If applicable, provide a discussion of how the Offeror might meet any unmet performance goals under a future effort. This final report must also include “lessons learned” from the effort, recommendations for future research, development, or testing that would lead to success in meeting the performance goals. The final report must provide a comprehensive and detailed account of all funds expended.

## **14. OTHER INFORMATION**

### **Government Furnished Property (GFP), Government Furnished Equipment (GFE) and Facilities**

Each Offeror must provide a specific description of any equipment/hardware that it needs to acquire to perform the work. This description must indicate whether or not each particular piece of equipment or hardware will be included as part of a deliverable item under the resulting award. This description must identify the component, nomenclature, and configuration of the equipment/hardware that it proposes to purchase for this effort. The Government strongly prefers that contractors purchase the equipment or hardware for deliverable items under an award. Other arrangements, leading to GFP, will be considered on a case by case basis. Maximum use of Government integration, test, and experiment facilities is encouraged.

Government research facilities may be available and must be considered as potential government furnished equipment/facilities. These facilities and resources are of high value and some are in constant demand by multiple programs. It is unlikely that all facilities would be used for any one specific project or program. The use of these facilities and resources will be negotiated as the program unfolds. Offerors shall explain which of these facilities they recommend and why.

### **Project Meetings and Reviews**

Program status reviews may also be held to provide a forum for reviews of the latest results from experiments and any other incremental progress towards the major demonstrations. These meetings will be held at various sites throughout the country. For costing purposes, Offerors shall assume that 40% of these meetings will be at or near DHS S&T offices in Washington, DC and 60% at the contractor’s offices or other government facilities. In any event, all travel shall be done in accordance with the Federal Travel Regulations. Interim meetings are likely, but these will be accomplished via video telephone conferences, telephone conferences, or via web-based collaboration tools.

## **SAFETY Act**

Congress enacted the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (the "SAFETY Act") as part of the Homeland Security Act of 2002. The SAFETY Act provides limitations on the potential liability of those firms that develop and provide qualified anti-terrorism technologies. DHS's Science and Technology Directorate, acting through its Office of SAFETY Act Implementation, encourage the development and deployment of anti-terrorism technologies by making available the SAFETY Act's system of "risk management" and "liability management." Offerors submitting proposals in response to this BAA are encouraged to submit SAFETY Act applications on their existing technologies and are invited to contact the Office of SAFETY Act Implementation (OSAI) for more information at 1-866-788-9318 or [helpdesk@safetyact.gov](mailto:helpdesk@safetyact.gov) or visit OSAI's website at [www.safetyact.gov](http://www.safetyact.gov).

**APPENDIX 1**  
**S&T LONG RANGE BAA 14-02 White Paper Format**

Offerors shall not exceed 5 pages total using this format.

*The government reserves the right to reject  
submissions in excess of 5 pages.*

Name of Project/S&T Division
Name(s) and Contact Information of Performers
Name (Citizenship): Mailing Address: Telephone: Email:
Name and Contact Information of Financial Contact
Name (Citizenship): Mailing Address: Telephone: Email:
Overall scientific and technical merits of the Proposal /Mission Relevance
Estimated Duration of Project (From Award Date)
Estimated Total Project Cost
Offeror's capabilities, related experience, and past performance, including the qualifications, capabilities, and experience of the proposed principal investigator and personnel. Resumes are not requested but qualifications must be included.

**APPENDIX 2**  
**S&T LONG RANGE BAA 14-02**

**INTELLECTUAL PROPERTY CHART TEMPLATE**

<b>List Technical Data Computer Software to be Furnished with Restrictions</b>	<b>Provide a Summary of Intended Use in the Conduct of the Research</b>	<b>List Basis for Assertion</b>	<b>List Asserted Rights Category</b>	<b>Provide Name/Title of the Person Asserting Restrictions</b>