

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:

BMD	sandt.bordersmaritime@hq.dhs.gov
CDS	standards@hq.dhs.gov
CSD	sandt-cyber-liaison@hq.dhs.gov
EXD	sandt.explosives@hq.dhs.gov
FRG	sandtfrg@hq.dhs.gov
RSD	sandt.rsd@hq.dhs.gov

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

S&T BAA Website Tech Support: dhsbaa@reisystems.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 Division Director 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 Division Director 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 Division Director 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 Division Director 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 Division Director. The Division Director 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 Division Director may require additional relevant information from the Offeror. The Division Director 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 LRBAA 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 LRBAA. 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) LRBAA 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.

Land Border Security

Detection of, tracking of, classifying of, and responding to all threats along the terrestrial border between the Ports of Entry, specifically technologies that can perform one of the following functions:

BMD 1.1 - Noninvasive, minimally disruptive sensors and systems that can detect and locate clandestine, unknown subterranean threats (tunnels and other objects of interest to law enforcement) within varied geologies of the southwest border.

BMD 1.2 - 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
- Enabling technologies that will allow tactical, low-altitude unmanned aircraft systems to be operated safely, securely, and responsibly in the National Airspace System
- Strategies for long-term and economical operations and maintenance of unmanned aircraft systems, such as innovative uses of modularity, spares, and power management

BMD 1.3 - Small, covert sensors for detection and classification of personnel day and night. Low false/nuisance alarm rates and long battery or renewable energy lifetimes of a minimum of 6 months. Capability to exfiltrate information.

BMD 1.4 - Sensors for detection and/or tracking of personnel in dense foliage day and night. Estimated procurement costs versus area coverage is an important consideration. Capability to exfiltrate information and suitable for four season weather. Battery or renewable energy lifetimes of a minimum of 6 months.

BMD 1.5 - Border Illegal Flow Pattern Recognition: Technology which accesses multiple data sets and applies an algorithm to identify existing patterns of border illegal flows, along with the confidence index of the correlation. An example of stimuli and outcomes could be there is a 90% correlation of decreased violence along the land border with increased interdiction rates. This would enable DHS to understand the threat landscape and potential use it has a basis for predictive analytics.

BMD 1.6 – Border Illegal Flow Prediction: Technology which accesses multiple data sets and applies an algorithm to predict where border illegal flows will shift under different circumstances, along with the confidence index of the prediction. An example of stimuli and outcomes could be there is a 95% confidence level increased enforcement action at ports of entry resulting in illegal flows shifting to the land between ports of entry in the immediate vicinity. This would enable DHS to ensure that resources between ports of entry are increased in the vicinity whenever increased enforcement actions at ports of entry are occurring.

BMD 1.7 – Border Illegal Flow Risk Assessment: Technology which accesses multiple data sets and applies an algorithm or suite of algorithms to analyze the vulnerabilities for border illegal flows based on force structure, along with the confidence index of the prediction. An example is exploring the resource allocation of agent patrols vs. technology surveillance assets for patrolling various zones, based on their detect/identify/track capabilities along with the need to execute interdiction actions. This would enable DHS to analyze multiple force laydowns in response to various threat environments and determining optimal resource allocation that would drive current deployment along with strategic planning.

BMD 1.8 – Forensic Analysis Tools: Technologies and methods to efficiently collect, analyze, and identify forensic properties such as pollen, material types, fingerprint, DNA, isotopic, and others.

BMD 1.9 – Counter Unmanned Ariel Systems (CUAS) Detection, Track, and Classification: Unmanned Ariel Systems can represent a threat to people, critical infrastructure, and border alike.

Technologies and methods to detect, track, and classify UAS's in complex environments, including the determination of intent. Proposals can be submitted to test existing systems or to develop an advanced capability.

BMD 1.10 - Unmanned Ariel Systems Mitigation: Conventional weapons have been designed to locate and destroy targets; however, none have been developed and used to engage small, slow, maneuverable UASs in a complex and populated environment. Technologies and methods to detect, track, and classify UAS's in city environments, including the determination of intent. Proposals can be submitted to test existing systems or to develop an advanced capability. Proposals can be submitted to test existing systems or to develop an advanced capability.

BMD 1.11 - This program develops technologies to enhance security while expediting the flow of legitimate trade and travel. The program will work to reduce the risk of terrorists and transnational criminal organizations from exploiting lawful international travel, cargo and conveyances for illegal smuggling of people and contraband. The program will also take a cost effective approach to implementing technologies and capabilities to ensure the security and expediency of travelers entering and exiting the U.S.

BMD 1.12 - Analyze current operations, and implement technologies and process enhancements to existing airport operations, to increase CBP's capability to expedite screening of travelers. Develop recommended approaches and implement improvements in processes and/or technologies for cost-effective and integrated biometric, biographic, behavioral, or other capabilities to support transformation of the inspection process and facilitate increased travel and tourism. This will include, but is not limited to, traveler queuing optimization, enhanced/improved screening tactics/techniques/procedures, next-generation Federal Inspection Service inspections, development of inspection metrics and analytics, integrated customs and agriculture baggage inspection, and evaluations of officer-systems performance.

Maritime Border Security

Promising maritime border security capabilities defined in the following categories will be required to demonstrate suitability of use including ease of connectivity and operational effectiveness. S&T is developing the Coastal Surveillance System (CSS) which employs open standards and selected technologies/capabilities/concepts must ensure connectivity to the CSS enterprise architecture and will undergo an interoperability assessment.

BMD 2.1 - Improved visualization and tools - enhancements to industry standard Ozone Widget Framework (OWF), common operating picture and toolset to incorporate new capabilities and provide better cross-domain support.

BMD 2.2 - Improved situational awareness by automated or assisted behavior analysis and alerting - 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.

BMD 2.3 - Improved quality of data, via sensor performance or near real-time processing to enable improved detection and tracking of small and large vessels by overcoming environmental clutter issues within the port/harbor as well as coastal environments.

BMD 2.4 - 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.

BMD 2.5 - Improved communication devices or methods to enable simplified sharing of selected radar, video, and other information to tactical commanders.

CAPABILITY DEVELOPMENT SUPPORT (CDS) – OFFICE OF STANDARDS

CDS Office of Standards provides technical assistance and policy guidance to the DHS Components on the development of voluntary consensus standards that meets their needs. Standards support the development of consensus-based measures- from basic specifications to performance criteria – that give DHS and its customer’s confidence that technology and systems will perform as required. CDS Office of Standards works across DHS and with external partners to build consensus and encourage the adoption of needed, voluntary standards.

CDS.01 – Accelerate the development and integration of consensus standards by researching and identifying standards gaps and developing road-maps and integration plans for development of standards in the areas of Digital Imaging and Communication Security, Response Robots to Nuclear Power Incidents, and First Responder standards.

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 for Cyber Security Experimentation - Effective, strongly grounded experimental research forms a key element of CSD’s strategy to address the nation’s critical cyber security challenges. To catalyze and support such research, CSD seeks to develop advanced experimental research tools, technologies, methodologies and infrastructures as broadly available national resources. Key to the success of this program objective will be the realization of experimental research infrastructures, capabilities, and approaches that reach beyond today’s state of the art. These infrastructures, together with similar broad-based objectives that transform discovery, validation, and ongoing analysis in an increasingly complex and challenging domain must provide, as examples:

- Support for multi-disciplinary, complex, and extreme scale experimentation;
- Support for emerging research areas such as specialized cyber-physical systems and

cybersecurity relevant human behavior;

- The creation and capture of advances in scientific methodologies, experimental processes, and education; and
- Strategies for dynamic and flexible experimentation across user communities and infrastructure facilities.

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 - seeking architectures, technical approaches, studies, processes, technologies, tools and other efforts to improve the security and determine and mitigate the vulnerabilities of:

- authentication and identification technologies as applied to people and non-person entities
- novel approaches to implement fraud analytics and compensating controls to mitigate risk
- risk based approaches to identity resolution, validation and verification
- ensuring integrity and confidentiality of data as it traverses multiple environments such as mobile, cloud, internet and enterprise networks
- access control and authorization technologies to manage access to data and resources.

Identity Management research projects will seek to develop, test, and evaluate the feasibility, interoperability, usability, vulnerabilities, standards conformance and other factors across this broad domain to increase security and productivity while decreasing costs and security risks.

CSD.06 – Data Privacy Technologies - seeking architectures, technical approaches, studies, processes, technologies, tools and other efforts to:

- manage personally identifiable information or information deemed sensitive in a manner that protects individual privacy
- automate control of privacy data to minimize cognitive overload while minimizing privacy risk
- understand and address privacy concerns with connected devices and sensor platforms a.k.a. internet of things
- understand and address privacy concerns with the use of big data and algorithms
- understand and address privacy implications and effectiveness of security screening measures

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. To address this objective, CSD is seeking research in areas such as: software analysis techniques for vetting untrustworthy software to address Software Supply Chain Risk Management; secure coding techniques to assist developers with software

development activities to improve coding practices; mobile app vetting capabilities; binary analysis capabilities; and formal methods used for specification, development, and verification of software systems.

CSD.08 – Cyber Security Education – objective is to develop, demonstrate and transition substantive and adaptive cyber security education models that impact organizations and infrastructures/sectors for the better. These models should address key dimensions of the challenge, such as multiple age levels, cyber security across multiple operational domains, and different kinds of threats. An overarching objective of this work is to support development of “learning organization” capabilities across all kinds of organizations and infrastructures/sectors. The models and associated technologies need to support cyber security competitions, education and curriculum development, and workforce training and development needs. To address this objective, CSD anticipates cyber security research in areas such as:

- the coupling of operations with education and training;
- abstract learning versus learning with context;
- Bayesian learning (prior knowledge) and where and how it might be applicable;
- Incident response feedback systems, that drive subsequent training/learning directions;
- Regional education and learning models coordinating efforts across different kinds of organizations.

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 into the areas of: cybersecurity insurance and cyber behaviors (individual and organizational; criminal or terrorist in nature)

- 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
- e) Cyber insurance and liability

CSD.15 – Data Analytics – The exponential increase in the volume of data created and transmitted worldwide over interconnected and interdependent cyberinfrastructures creates new challenges for cyber security. S&T is interested in technologies and tools to support the analysis of datasets whose size and complexity are beyond the ability of commonly used software tools to capture, manage, process, and interpret. These include but are not limited to:

- Threat discovery
- Automated or real-time analysis techniques
- Machine and self-learning algorithms
- Data visualization
- Resilience of physical and societal infrastructures to cyber threats

CSD.16 – Predictive Analysis-- Predictive Analysis, as applied to cyber security, is the ability to identify potential cyber threat vectors and determine the probable course of action for each threat. These findings should be presented automatically, with human-in-the-loop if desired, but not required. Presentation should be in an easily understandable format, to allow resource management to address threats as they evolve. Predictive Analysis may be applied at any phase or stage, from fully protected to compromise and recovery. All types of cyber threats may be considered.

CSD.17 - Distributed Denial of Service Defense – Denial of service attacks are pervasive and have the potential to disrupt critical network infrastructure. Topics of interest include:

- efforts that leverage existing policies and practices to mitigate DDoS attacks,
- techniques that adopt existing technologies for near term DDoS protection, and

- novel approaches for measuring and understanding DDoS attacks and new techniques for future DDoS mitigation.

CSD.18 – Cloud Computing Security – Research and Development to build upon security in cloud based systems—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.19 – Next Generation Cyber Infrastructure – CSD’s Apex project is focused on capabilities for use in Finance Sector environments, but they can be applicable across multiple sectors. CSD requires capabilities in the following areas:

- Advanced Sensing Technologies, to include technologies which verify the presence or absence of unauthorized modifications to endpoints and behavioral modeling
- Situation Understanding, to include technologies to correlate sensor alerts and human inputs and present relevant observations for improved human understanding and characterize networks and network topologies
- Response and Recover technologies, to include those that enable rapid, policy-based execution of situation-specific responses (e.g. reconfiguring a sensor grid to clarify a situation)
- Advanced Network control planes, to include secure dynamic enclaves, secure routing, browsing and network essential services

CSD.20 – Anonymous Networks and Currencies—Tools and techniques to aid law enforcement in the investigation of cyber crimes committed using friend-to-friend networks, anonymous networks and/or cryptocurrencies.

CSD.21 – Cyber Situational Understanding—Research and development of operational technologies to provide situational understanding.

Situational understanding is more than reputation or situational awareness. Many individual tools are available that provide information or metrics that contribute to situational awareness. To achieve situational understanding, a broad view needs to be developed that incorporates many of these individual metrics, tools, or information items, and blends together data from many sources into very few, (possibly only one) tool or metric. When items of interest are identified, a drill-down capability will allow various actors in the cyber security field to gain the specific knowledge needed for actionable intelligence. In some ways this can be viewed as an integration task, to identify, correlate and blend data from various sources to make it understandable and usable not only to cyber security professionals, but to others (from management and decision makers to consumers) affected by cyber security incidents.

CSD.22 – Research Data Marketplace – CSD seeks to coordinate, enhance and develop advanced data and information sharing tools, datasets, technologies, models, methodologies and infrastructure to support national and international cyber risk research. These data sharing components are intended to be broadly available as national and international resources to support the three-way partnership among government, critical information infrastructure providers, and network & cybersecurity R&D communities. A primary goal is to bridge the gap between producers of cyber-risk-relevant operations data, academic and industrial researchers, and technology developers to inform policy and analysis of cyber-risk and trust by:

- creating deeper and broader networks of information sharing;

- fostering the development and adoption of automated mechanisms for information sharing; and,
- accelerating the understanding of issues and the design, production, and evaluation of solutions

EXPLOSIVES COUNTERMEASURES DIVISION

Explosives Countermeasures include the detection, mitigation, and response to explosive threats in all modes of transportation (Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline). The Explosive Countermeasures Division seeks to improve detection, response, and defeat capability for homemade explosives (HME); improvised explosive devices (IEDs), vehicle borne (VBIED) and person borne improvised explosive devices (PBIED).

EXD.01 – Standoff Detection of Explosives: Technologies for the standoff detection of explosives and explosive devices related to PBIEDs and VBIEDs. The ideal system would detect diverse explosive signatures, including commercially available explosives, military explosives, and HMEs. Standoff Detection implies that both the detection equipment and operator are 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.
- (2) Automated detection and/or identification capabilities associated with both imaging and spectroscopy.

EXD.02 – Trace Detection of Explosives: This subtopic includes detecting the broadest possible range of trace particle and vapor signatures in aviation security, facility 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, advanced ETD system concepts, and technologies that improve sampling from passengers (e.g., hand swipes), clothing, baggage, and personal items such as electronic devices.

EXD.03 – Cargo Security:

Technologies proposed for cargo security must be cost-effective, high-throughput, and capable of efficiently processing incoming cargo spanning the range of sizes encountered in that mode of transportation.

EXD.04 – Data Fusion and Automated Detection for aviation cargo, checked baggage, carry-on baggage, personal check points and all surface intermodal concerns. Algorithms and techniques are particularly desired 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 Advanced Imaging Technology (AIT) for the screening of passengers and video. Automated Target Recognition algorithms suited for analyzing real-time inputs from video-rate data (video, AIT, or other sources) are of particular interest.

EXD.05 – Advanced Detection Technologies: Development of robust, enhanced explosives detection methods to improve selectivity and sensitivity capabilities. Detection methods should be easily deployed, low cost, and require minimum training to operate. Technologies that

provide orthogonal, secondary screening to resolve alarms in checked baggage or checkpoint scenarios are of special interest.

EXD.06 – Risk-Based Screening: Proof-of-concept demonstrations of hardware and/or software-based methods that can intelligently adjust parameters such as alarm thresholds in response to a change in threat level. Of particular interest are methods that could integrate screening data from multiple systems to reach an integrated threat decision.

EXD.07 – Improved X-Ray System Components: This subtopic includes but is not limited to superior X-Ray sources, collimation methods, other optical components, detectors, and any software or algorithms required to operate and interpret the data produced. Techniques that extract additional information (data regarding multiple energies, diffraction, phase, etc.) during X-Ray screening are of special interest.

EXD.08 – Canine Explosive Detection Technologies: Development of non-hazardous HME and conventional explosive training aids with a specific focus on pure odor materials, not pseudo scents or tagged odors. Operational efficacy, safety and cost are major metrics of success. Technologies and methodologies that advance the capture of canine performance in controlled and operational environments representative of the expanse of the Homeland Security Enterprise at the federal, state and local level and facilitate scientifically significant data capture through independent operational test and evaluation. Specific focus on protocols that facilitate the reduction in the number of trained odors required for comprehensive canine explosive detection proficiency.

EXD.09: Homemade Explosives: Develop threat information for HMEs such as intelligence related or hazard validation data and risk-based analysis tools. Develop technologies to inhibit the unlawful use and manufacture of HMEs, such as, precursor inhibitors to reduce the likelihood of use in an HME by eliminating the ability to weaponize a precursor while maintaining its original intent and safe use. Develop desensitization techniques of HME materials for safe movement and response measures for large volume disposal operations such as when HME is not containerized in domestic facilities to reduce the cost of public and private property damage. Develop response tools to impart energy but not detonate more sensitive HMEs such as TATP or HMTD.

Apex Screening at Speed

This portfolio covers the screening of passengers, their personal items, their carryon bags and associated secondary screening for an airport security checkpoint of the future. The checkpoint of the future, planned to be deployable in five years, seeks to improve passenger experience while enhancing detection capabilities. Specifically,

EXD.10.1 – Checkpoint Passenger Screening: EXD invites white papers on technologies that allow for screening three hundred or more passengers per hour with minimal need for divestiture of headwear, footwear or personal items while providing detection up to the Transportation Security Administration's (TSA) Tier IV security detection standards. The systems should be capable of being able to adapt, or upgrade, quickly to respond to emerging threats.

EXD.10.2 – Checkpoint Baggage Screening: EXD invites white papers on technologies that allow the processing of up to 600 bags per hour, without the need to divest laptops, liquids, aerosols, or gels from the bag being screened. Systems will have to meet TSA's Tier IV detection standards.

EXD.10.3 – Special Purpose Screening: EXD also invites white papers on screening technologies that address niche detection requirements or secondary screening of passengers or their articles. Such technologies might include nuclear quadrupole resonance (NQR), non-contact or automated trace detection, and technologies that support the screening of items and people that alarm during the primary screening process.

EXD.10.4 – Algorithms & Software: EXD invites submissions pertaining to algorithms and software that will allow integration of sensors such as application programming interfaces (API's), vendor independent detection algorithms, and test beds that can be used to evaluate compliance with Digital Imaging and Communications in Security (DICOS V02) and similar standards.

The Technologies developed under EXD.10.1 through EXD.10.4 should be compatible with standards and protocols in common use in aviation security, including but not limited to DICOS V02, TSA's Security Technology Integrated Program (STIP), and TSA's Dynamic Aviation Risk Management System (DARMS) initiatives. Offerors should include provisions for providing a prototype of the associated hardware to a Government laboratory chosen by EXD for test and evaluation.

FIRST RESPONDERS GROUP

The First Responders 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 First Responders Group 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; (4) overseeing the National Urban Security Technology Laboratory, which provides a test and evaluation capability for DHS-developed technologies and systems; and (5) providing an assessment program for commercially available and emerging technologies.

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.04 – 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.08 – Flood Forecasting/Modeling: The ability to monitor the level of precipitation, runoff, and river water levels and flow rates for simulation and a minimum of five day flood forecasting, with daily update capability, and more frequently during actual floods. Improvements in this capability can: (1) Integrate new modeling methodology and/or very low cost sensors; (2) Localize water forecasts to specific geographies/known flood prone areas; (3) Integrate with the National Response Framework; 4) Work for both flood and drought; and (5) Integrate with FEMA’s Integrated Public Alert and Warning System (IPAWS) or other Public Statewide or local alerting systems.

FRG.09 – Community Resilience: The ability to use behavior-based methods, models, trainings and technologies to enhance community resilience in the face of human- or nature-caused catastrophes. Improvements in this capability can include: (1) Better understanding of risk perception; (2) Improved risk communication by emergency responders and public officials; (3) Pre-event education and training methods; and (4) Applied theoretical and empirical research into the properties of resilient social networks and communities to include elements of social media and crowd sourcing.

FRG.10 – Violent Extremism: The ability to counter violent extremism improvements can include: (1) Research and development to improve the detection, analysis, understanding, and mitigation of the threats posed by violent extremists; (2) Knowledge, tools and technologies to determine when individuals, groups, and movements are likely to engage in violence; and (3) What ideological, organizational, and contextual factors may influence violent action.

FRG.11 – Resilient and Sustainable Infrastructure: The ability to enhance security, resilience, and recovery of the 18 critical infrastructure sectors for retrofit applications. Developing infrastructure that is resilient and 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. Improvements in this this area include: (1) 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; (2) 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; (3) Key critical infrastructure component design that use high-performance green materials that are self-monitoring, self-healing, provide greater longevity than current materials; and should resist blast, earthquake, floods, and wind.

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@reisis.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 Kyle Graumann at DD254ADMINISTRATIVESECURITY@HQ.DHS.GOV.

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. 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* and *unclassified* submissions should be sent to Kyle Graumann at DD254ADMINISTRATIVESECURITY@HQ.DHS.GOV and to s&t-2014-lrbaa@hq.dhs.gov **before** emailing classified information to DD254ADMINISTRATIVESECURITY@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.
- ✓ 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 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.

Science & Technology Directorate
U.S. Department of Homeland Security

- **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 LRBAAs 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

Science & Technology Directorate
U.S. Department of Homeland Security
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

Science & Technology Directorate
U.S. Department of Homeland Security

(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 LRBA 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 LRBA 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 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 and 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. 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 or visit OSAI's website at 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

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