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 11-03
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 announcement will remain open until December 31, 2011 at 11:59 PM Eastern. White Papers and Full Proposals may be submitted at any time while the announcement is open.

Points of Contact:

W. Adrian Groth
LRBAA Coordinator
Department of Homeland Security
Science & Technology Directorate
245 Murray Lane, SW
Mail Stop 2100
Washington, DC 20528-2100
LRBAA.Admin@hq.dhs.gov

Michael Gruden
Contract Specialist
Department of Homeland Security
Office of Procurement Operations
245 Murray Lane, SW
Mail Stop 0115
Washington, DC 20528-0115
LRBAA.OPO@hq.dhs.gov

S&T BAA Website:	https://baa2.st.dhs.gov
S&T BAA Website Tech Support:	dhsbaa@reisys.com or (703) 480-7676

2. INTRODUCTION

This is a Long Range Broad Agency Announcement (LRBAA), as contemplated in Federal Acquisition Regulation (FAR) 6.102(d)(2) and 35.016. Its distinctive requirements are different from those of targeted BAAs. The Department of Homeland Security (DHS) Science & Technology Directorate (S&T) reserves the right to reject submissions that do not comply with the submission instructions contained in this document. Please read them carefully.

This Announcement declares S&T's broad interest in competitively funding R&D projects across a spectrum of science and engineering disciplines. These projects relate to revolutionary, evolving, and maturing technologies that demonstrate the potential for significant improvement in homeland security missions and operations. S&T will focus on areas where risk inhibits mission or operational investments, and where significantly improved or increased capability payoffs can be expected.

In summary, any Offeror who believes his or her project satisfies the criteria described in this Announcement may submit a White Paper. Upon review, the Contracting Officer, after consultation with technical expert S&T personnel from the relevant division, may encourage the Offeror to submit a Full Proposal. This document describes these requirements and processes.

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 topics and topical areas of interest beginning on page 6, which correspond to S&T divisions, and identify the specific division where their concept will have the maximum impact. Offerors are encouraged to select the one division that most directly corresponds to their proposed subject matter.

Offerors must clearly articulate in submissions their specific advances or innovations. 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 LRBAA is not a request for information (RFI). The submission and evaluation process for this LRBAA is distinct from those of conventional procurements that use Requests for Proposals (RFPs) or Requests for Quotes (RFQs).

Offerors should be aware that there are typically several other DHS Broad Agency Announcements open, in addition to this LRBAA. These BAAs are targeted at individual topical areas. The targeted BAAs and the LRBAA may be accessed online at https://baa2.st.dhs.gov.

The mission of DHS S&T 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." As such, 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. 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 LRBAA award shall be primarily for the purchase of capital equipment.

Offerors who seek, through this LRBAA, 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 LRBAA. 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 LRBAA.

DHS S&T will not issue paper copies of this Broad Agency Announcement.

3. ELIGIBILITY INFORMATION

All responsible Offerors are eligible to submit White Papers under the LRBAA, 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 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 LRBAA 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.

Independent organizations and teams are encouraged to submit 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 Contracting Officer will consult with technical expert S&T personnel from the relevant divisions and identify White Papers that present "particular value" to S&T. The 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.

DHS S&T reserves the right to select for award and fund all, some, or none of the Full Proposals received in response to this Announcement. If an award decision is made, funding will then be determined through a negotiation process. 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 LRBAA. Awards will be made based on an assessment of the White Paper or Full Proposal's particular value to the Government. Awards will be made based on proposal evaluation, funds availability, and other programmatic considerations. Awards may take the form of contracts, grants, cooperative agreements, or Other Transaction Agreements (OTA). Please note that as of the writing of this document, DHS S&T's other transaction authority has sunsetted on September 30, 2010 and has not been reinstated. Any awards based on other transaction authority may not be made until the authority is reinstated by Congress.

The applicable laws and regulations governing a particular award will depend on that award vehicle. 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 those cases, S&T will leverage those technology developments wherever it is practicable and efficient to do so. S&T will also facilitate access to laboratory and operationally relevant test and evaluation facilities, where reasonably available.

5. ETHICAL CONSIDERATIONS

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

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

During the evaluation period, the LRBAA Contracting Officer must be the focal point of any exchange with Offerors. A Contracting Officer may initiate communications if and when specific facts in the submission require further clarification (such as confirmation of a delivery date). If the Offeror receives a notification letter encouraging the submission of a Full Proposal, communications may ensue between S&T and the Offeror regarding scope of work, resources required to execute the scope, etc., provided that a Contracting Officer is present for such discussions. **No exchange related to price is allowed.**

Conflict of Interest: 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 and include a mitigation plan for any actual or potential conflicts of interest, in accordance with paragraph (c) of this provision.

(b) Determination. The Contracting Officer may determine that this effort may result in an actual, potential, or perceived conflict of interest.

(c) If an Offeror with an actual, potential, or perceived conflict of interest believes it can be mitigated the Offeror may submit a mitigation plan to the Contracting Officer. The Contracting Officer may approve a mitigation plan; reject a mitigation plan and ask for revisions; or reject a mitigation plan, determine that the conflict of interest cannot be resolved or avoided, and find the Offeror ineligible for award.

(d) Other Relevant Information. In addition to the mitigation plan, the Contracting Officer may require additional relevant information from the Offeror. The Contracting Officer will use all information submitted by the Offeror, and any other relevant information known to DHS, to determine whether an award may be made and whether the mitigation plan adequately mitigates the conflict.

(e) Corporation Change. The successful Offeror shall inform the Contracting Officer, within 30 calendar days of the effective date of any corporate mergers, acquisitions, or divestitures that may affect this provision.

(f) Flow-down. The contractor shall insert the substance of this clause, paragraphs (a) through (f), in each subcontract that exceeds the simplified acquisition threshold.

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

Federal Acquisition Regulation (FAR) provision incorporated by reference:

FAR 52.209-2 Prohibition on Contracts with Corporate Expatriates – Representation
Note: Actual awards will incorporate Homeland Security Acquisition Regulation (HSAR) clause (deviation) 3052.209-70 Prohibition on Contracts with Corporate Expatriates.

6. PRE-SUBMISSION INQUIRIES

Prior to preparing and submitting White Papers, potential Offerors may submit informal inquiries to the S&T division that best matches their proposed concept. S&T personnel cannot assist in the preparation of a White Paper, nor can they propose any ideas they would like potential Offerors to address. S&T personnel can indicate whether an idea appears to be within the scope of the division's interests and within the scope of this LRBAA. All White Papers and Full Proposals must be submitted through the BAA website https://baa2.st.dhs.gov; they shall not be sent to the division email addresses. These S&T division email inboxes are monitored regularly.

Pre-submission inquiries shall include a brief description of the technology, the proposed research, how it is new and different from what is currently available, and its proposed applications. Fully developed products are not considered under this LRBAA unless the Offeror is proposing a totally different application for the product or a modification is needed and some research is required to determine if it will be successful.

A pre-submission inquiry may consist of no more than a single page and must use Times New Roman 12-point font. Most pre-submission inquiries will come via email, and this same length limit applies to email.

Offerors may submit a White Paper to the LRBAA irrespective of the feedback obtained from a pre-submission inquiry.

DHS S&T Divisional Points of Contact

Emails sent to the contacts listed below shall indicate in the subject line: "Long Range BAA"

Borders and Maritime:	sandt.bordersmaritime@dhs.gov
Chemical/Biological:	sandt.chembio@dhs.gov
Cyber Security:	sandt-cyber-liaison@dhs.gov
Explosives:	sandt.explosives@dhs.gov
First Responders:	sandtfrg@dhs.gov
Human Factors/Behavioral Sciences:	sandt.hfd@dhs.gov
Infrastructure Protection and Disaster Management:	sandt.idd@dhs.gov
HSARPA/Innovation:	sandt.innovation@dhs.gov

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

Topical Areas of strategic interest include:

BMD.01 – Border and Maritime Security focuses on tools and technologies that improve the security of our Nation's borders and waterways without impeding the flow of commerce and travelers. Concepts and prototypes of interest to the Borders and Maritime Security division include pilot testing new surveillance, monitoring, and response capabilities that cover vast expanses of remote border territories; as well as the development and evaluation of security devices, and new inspection methods to secure the large volume of cargo entering our Nation's ports daily.

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

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

- Objective 1.1: Increase ability to detect weapons of mass destruction and other illegal border activities while requiring less manpower
- Objective 1.2: Reduce agent response time
- Objective 1.3: Increase officer safety while securing the border and responding to border threats
- Objective 1.4: Increase officer capability to rapidly verify the identity of illegal immigrants

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

- Objective 2.1: Develop and demonstrate visual and non-visual technologies for monitoring the maritime border
- Objective 2.2: Enhance the ability of law enforcement to quickly detect and localize maritime threats and provide timely decision-support information

Goal 3: Develop technologies to reduce the risk of illegal drugs, contraband, currency, weapons of mass destruction, and illegal immigrants from transiting to the U.S. via cargo channels.

- Objective 3.1: Provide capability to ensure the physical integrity of cargo shipments (including sea, air and land conveyances)
- Objective 3.2: Increase supply chain visibility through tracking and chain-of-custody monitoring
- Objective 3.3: Increase the detection of suspect cargo shipments and activities of interest in shipping containers

There are 3 subdivisions within Border and Maritime Security: Land Border Security, Maritime Border Security, and Cargo Security.

A. Land Border Security

BMD.02 – Detection of, tracking of, classifying of, and responding to all threats along the terrestrial and maritime border – in particular, technologies that can:

- Classify humans versus animals in rugged terrain, concealing foliage, water obstacles, mountains, and other environmental constraints
- Lower false alarm rate (Pfa) with raised probability of detection (Pd); Pd should be at least 90%
- Operate at low power consumption levels (2 year battery life)
- Detect, exploit, interrogate, and remediate subterranean border tunnels
- Detect and track low-flying threat aircraft

BMD.03 – Improved analysis and decision-making tools that aid DHS watchstanders in evaluating information and making more timely and accurate decisions.

BMD.04 – New and improved airborne sensors, including persistent, wide-area surveillance capabilities, for better land border security to assist in locating illicit activities, materials, or their means of conveyances.

BMD.05 – Enabling technology for securing the Nation's borders.

B. Maritime Border Security

BMD.06 – Provide wide-area surveillance from the coast to beyond the horizon, as well as port and inland waterways, for detection, classification, tracking, and response.

BMD.07 – New and improved airborne sensors, including persistent, wide-area surveillance capabilities, for better maritime border security to guard U.S. coastal approaches from 12 to 120 miles offshore and to assist in locating illicit activities, materials, or their means of conveyances.

BMD.08 – Improved situational awareness by tracking small boat activity, detecting anomalous and/or illegal behavior, and providing timely and actionable information in support of law enforcement and port security efforts.

BMD.09 – Improved sensor performance to enable improved detection and tracking of small and large vessels by overcoming environmental clutter issues within the port/harbor as well as in coastal environments.

BMD.10 – Advanced law enforcement capabilities, enhanced ability to protect critical infrastructure and key resources, and improved incident response and recovery management along the inland waterways, port/harbor, and coastal regions.

BMD.11 – Concepts, methodologies, and/or technologies to more effectively track dangerous cargo being transported on inland rivers and waterways.

BMD.12 – Improved data fusion and automated tools for command center operations – in particular, the improved ability for agencies to share information and collaborate when not co-located.

C. Cargo Security

BMD.13 – Improved screening and examination by non-intrusive inspection – in particular, the ability to detect or identify contraband items (for example, drugs, money, illegal firearms), threat materials, or stowaways; improve penetration, resolution, throughput, contrast sensitivity, reliability, mobility, and interoperability; and integrate with future Automated Target Recognition capability.

BMD.14 – Increased information fusion, anomaly detection, Automatic Target Recognition, and response capability – in particular, automated imagery detection capability for anomalous content (e.g., stowaways, hidden compartments, contraband), and the ability to detect anomalous patterns in shipping data.

BMD.15 – Improved detection, and identification of WMD materials and contraband – in particular, the ability to detect chemical and biological threats, explosives, and contraband.

BMD.16 – Detect intrusion or unauthorized access, positively identify cargo, and provide timely response – in particular, in containerized, palletized, parcel, or bulk/break-bulk maritime and air cargo.

Chemical and Biological Division

CBD.01 – The Chemical and Biological Division performs analyses and countermeasures, including improved characterization and prioritization of threats, innovative or revolutionary methods for surveillance and detection for early attack warning that minimize exposure and speed treatment of victims, new forensic methods to support attribution, and novel concepts for decontamination and restoration, agro-defense, and food defense. It is important to note that the division does not fund research on human clinical applications.

Chemical and Biological R&D areas of strategic interest:

CBD.02 – Improved Informatics and Design for Biological and Chemical Analysis:
(1) Bioinformatics and chemical analytics research that leads to significantly higher success rates for assay design.
(2) Research to improve the depth and speed of data analysis and enhance access to (and indexing of) large datasets; particularly bioinformatics data structures as well as genotypic and phenotypic data.

CBD.03 – Improved Sampling:

(1) Research in the areas of biological particle capture and "real-time" analysis to support future development of technology that distinguishes between putative threat and non-threat agents.
(2) Research that develops fundamental understanding of sample collection from various surface types and matrices (e.g. air, water, Soil) to improve selectivity.
(3) Research that improves transfer efficiency of agents from the environment to detectors or instruments.
(4) Research that improves organism collection and preservation by 70% viability or greater.

CBD.04 – Sample Preparation:
(1) Research that improves the ratio of analyte of interest to background contaminant (AoI:BC) for chemical and/or biological threats; and
(2) Research that helps to improve and define the quality of samples that emerge from sample preparation in ways that are substantive to either instrumental or assay style analysis.

CBD.05 – Assays: Research to develop fundamental understanding and methodologies supporting assay chemistries that may potentially address the full spectrum of biological agents:
(1) traditional threat agents;
(2) agents that have been enhanced with known biological content;
(3) agents that have emerged via natural selection; and
(4) agents that are purely synthetic in nature.

Ultimately, this research should allow comparisons against highly flexible databases of information that enable unique identification of threat agents. Research toward assay chemistries that permit reliable differentiation between environmental contaminants and chemical/biological threat agents is also of interest.

CBD.06 – Instruments and Detection: Development, prototyping, and improvement of products and systems that are capable of detecting chemical and biological weapons, agents, and/or toxic industrial chemicals in aerosol, liquid, or environmental matrices, to support the following needs:
(1) Rapid detection and identification of an agent immediately after its release into the environment.
(2) Characterization and detection of novel, engineered, and emerging biological agents.
(3) Trace quantity detection of an agent to support decontamination efforts.
(4) Identification of a concealed agent or dispersal device prior to its release.

CBD.07 – Response and Recovery Research: Research aimed at enhanced understanding of chemical mechanisms and interactions with the environment and with operationally-relevant surfaces that will enable affordable and effective decontamination of emerging chemical threats and biological agents over wide areas.

CBD: Threat Characterization & Attribution

CBD.08 – Integrated Chem Bio Rad Nuclear Explosives (ICBRNE) Program: Prototype and pilot demonstration applications related to sharing of WMD sensor data and related information at the state, local, and federal level utilizing open standards and protocols.

CBD.09 – System Studies: Research to conduct studies and analysis to identify gaps in technology and operational concepts and to support formulation of requirements for chemical and biological countermeasure development. Current specific areas of interests are transit system defensive architectures and surveillance architectures to detect and/or characterize a biological attack.

CBD.10 – Bioforensics R&D Program: Supports research and development of next generation and novel technologies to characterize biological threat agents (BTAs) for source attribution in support of FBI/NBFAC requirements in a criminal investigation. These include novel applications of next generation technologies to characterize the organism or the sample matrix. Please refer to specific BAA releases for future submissions.

CBD.11 – CBRN Threat Characterization Program: Supports research and development of next generation and novel methodological approaches to terrorism risk analysis, intentional attack analysis, scenario modeling and simulation to support the following needs:

(1) Risk Management;
(2) Cost Benefit Analysis and Resource Allocation;
(3) Development and evaluation of deterrence, preparedness, response and mitigation strategies;
(4) Behavioral modeling of adversary intentions and public response to CBRN terrorism events.

Agro Defense

CBD.12 – New or improved vaccines for foreign animal disease (FAD) viral pathogens affecting domestic livestock:

(1) New, molecular-based vaccine candidates that improve the onset of immunity and can differentiate infected from vaccinated animals.
(2) Novel immunostimulants, adjuvants, or agents with an immune-based mechanism of action that can improve vaccine efficacy and/or vaccine potency.
(3) New vaccines that can increase spectrum of cross-protection against related strains.
(4) New vaccines based on novel state-of-the-art technologies (e.g., nanovaccines, VLPs).
(5) New biological-based anti-viral therapeutics (small molecule drugs excluded) that can be used in combination with vaccines.

CBD.13 – New or improved rapid diagnostic tests that facilitate foreign animal disease (FAD) outbreak surveillance, response, and recovery in livestock:

(1) New laboratory-based high throughput, molecular-based antigen detection platforms with improved sensitivity and result time.

(2) New field deployable/point of care antigen detection platforms with improved sensitivity and result time.
(3) New tests that can detect FAD in clinical samples (milk, blood, oral/nasal fluids) prior to onset of clinical signs.

CBD.14 – Efforts that address critical limitations in the current generation of foreign animal disease simulation models for high priority pathogens, including but not limited to the level of detail and parameterization required to adequately describe the diversity and complexity of the U. S. livestock system and the derived conceptual model, verification of the conceptual model versus its computer implementation, strategies for model validation versus the real world especially in a data poor environment, and the impact of data limitations at all levels of the modeling process.

CYBER SECURITY

CSD.01 – 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 Cybersecurity Initiative. These solutions include secure protocols, end system security, user identity and data privacy technologies, research infrastructure, law enforcement forensic capabilities, competitions, and education.

Cyber Security R&D areas of strategic interest:

CSD.02 – Internet Infrastructure Security – including Secure internet protocols including Domain Name System Security (DNSSEC) and Secure Protocols for Routing Infrastructure (RPKI and BGPSEC).

CSD.03 – Critical Infrastructure / Key Resources (CI/KR) Security and Resiliency – Technologies to support cyber security improvements in critical infrastructures within critical infrastructure sectors.

CSD.04 – National Research Infrastructure.

CSD.05 –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.06 – Cyber Forensics to support Law Enforcement.

CSD.07 – Information system insider threat detection models and mitigation technologies.

CSD.08 – Identity Management including technologies and standards for managing identities, rights and authorities used in an organization's information systems and networks.

CSD.09 – Data Privacy and Information Flow technologies.

CSD.10 – Software Assurance: Including tools and techniques for analyzing software vulnerabilities.

CSD.11 – Technologies to support cyber security competitions and education and curriculum development.

CSD.12 – Process Control Systems: Tools and technologies to secure process control systems and associated environments.

CSD.13 – Internet Measurement and Attack Modeling Techniques to enable better understanding of Internet security deployment and infrastructure (e.g., ASNs, routers).

EXPLOSIVES DIVISION

EXD.01 – Explosives Countermeasures include the detection, mitigation, and response to explosive threats including: all modes of transportation within the Transportation Systems Sector (Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline); in checked and carry-on baggage; Home Made Explosives (HME); improvised explosive devices (IEDs), vehicle borne (VBIED) and person borne (PBIED); and response and defeat technologies.

EXD.02 – Standoff Detection of Explosives: Technologies for the standoff detection of explosives and explosive devices related to Person and Vehicle Borne Improvised Explosive Devices. Explosives of interest include commercially available explosives (i.e. Ammonium Nitrate based), conventional military explosives (i.e. Composition C-4 and Semtex A/H) and homemade explosives (i.e., peroxide base). Standoff Detection implies that both the detection equipment and operator be located at some distance (>1 m up to tens of meters) away from the subject or object under interrogation. Subtopics include:

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

EXD.03 – Trace Detection of Explosives.

EXD.04 – Cargo Security includes detecting intrusion or unauthorized access, positively identify cargo, and provide timely response – in particular, in containerized, palletized, parcel, or bulk/break-bulk maritime, air cargo, and freight rail.

EXD.05 – Test and Evaluation Expertise and Facilities for Counter-IED detection technologies. Standoff, Remote, and Checkpoint based explosives detection systems, to be evaluated, most often require real explosives and local storage of said explosives. Facilities must be able to store, on-site, small amounts (< 1 pound) of various solid explosives, while achieving clean, uncontaminated facilities for equipment testing. Facilities must be able to accommodate

non-eye safe laser ranges, x-ray based screening equipment, and neutron-based screening equipment. Facilities must also be able to accommodate, in certain cases, large, outdoor vehicle borne IED screening equipment.

~~**EXD.06** – Defeat of Improvised Explosive Devices: Develop a means/method to attach an explosives access/neutralization charge to the external or internal surface of a vehicle or structure that is suspected of carrying or housing a terrorist explosive device. The means/method will allow for easy placement by a robotic platform, will allow for repositioning, and will support up to 100lbs. The means/method should be capable of adhering to glass, metal, wood, Fiber Reinforced Plastic (FRP), and concrete. Any means/method that proposes to use rope/ropelike items or double-sided adhesive tape is not acceptable.~~

~~**EXD.07** – Develop a tele-robotic manipulator that is capable of "fine motor" control for use in neutralizing an Improvised Explosive Device (IED). The system must be capable of precision actions such as cutting a wire, moving small components, opening small compartments, etc. The system must be mounted on or capable of being carried by a robot platform, is haptic sensitive, and weighs less than 25 lbs. The system should be self-powered, dual-armed and interoperable with the robotic platform Operator Control unit (OCU). The system should be capable of reaching up to 60."~~

EXD.08 – Data Fusion and Automated Detection for aviation cargo, checked baggage, carry-on baggage, personal check points and all surface intermodal concerns. Algorithms and techniques for detection fusion and automated alerting that combines a variety of detection modalities, including but not limited to X-Ray, trace chemical detection, computed tomography (CT) and video.

EXD.09 – Materials Science Research for Explosives Mitigation: Fundamental materials science research directed toward improved understanding of the relative importance and cumulative effect of aging, stress history, corrosion cracking, materials manufacturing variability and threats on critical infrastructure materials.

EXD.10 – Advanced Detection Technologies: Development of robust, enhanced explosives detection methods such as bio-inspired molecular recognition techniques and other advanced sampling technologies to improve selectivity and sensitivity capabilities. Detection methods should be easily deployed, low cost and require minimum training to operate. Special attention should be paid to determining better sensing mechanisms and signal amplification mechanisms to apply to future detection improvements.

FIRST RESPONDER GROUP

FRG.01 – The First Responder Group identifies, validates, and facilitates the fulfillment of First Responder capability gaps through the use of existing and emerging technologies, knowledge products, and the acceleration of standards. The FRG focuses on: (1) developing tools, technologies, methodologies, standards, protocols, and guidance to enable improved communications interoperability for First Responders; (2) providing First Responder solutions for high-priority capability gaps through rapid prototyping; (3) maintaining a Web portal that

enables First Responders to easily access and leverage Federal web services; and (4) overseeing the National Urban Security Technology Laboratory, which provides a test and evaluation capability for DHS-developed technologies and systems.

Alerts and Warnings

FRG.02 – Public Alerts and Warnings: Develops, evaluates, and establishes processes for the development of alert and warning systems to transfer a message from its origination point through the Federal government to the public on various devices. Tests and evaluates for development of a national capability to deliver relevant, timely, effective and targeted alert messages to mobile devices. Develops guidance to inform and engage the emergency response community in smart practices for utilizing social media capabilities to alert and warn the public.

FRG.03 – Public Response to Alerts and Warnings: Research, as part of the Commercial Mobile Alert Service (CMAS) research, development, testing and evaluation (RDT&E) program, to better understand how the public will respond to alert and warning messages. This clear understanding of the public's response will encourage consideration of the effect of geo-targeting, the 90-character limit proposed by the CMSAAC and supported by the FCC, and the effectiveness of message indicators when creating a message for public consumption.

FRG.04 – Multilingual Alerts and Warnings: Research, as part of the Commercial Mobile Alert Service (CMAS) research, development, testing and evaluation (RDT&E) program, to better understand how to ensure the same timely and effective access to alerts and warnings for the non-English speaking population that is made available to everyone else.

FRG.05 – Geo-targeting Best Practices: Research, as part of the Commercial Mobile Alert Service (CMAS) research, development, testing, and evaluation (RDT&E) program, to better determine when more granular geo-targeting, below the County level, is appropriate. Identification, testing, and evaluation of technologies that provide the capability of more granular geo-targeting. Work towards the acceleration of geo-targeting standardization, and the creation and establishment of best practices and standard operating procedures for adoption.

FRG.06 – Alerts and Warnings in Social Media Guidance: Definition of requirements and facilitation of effective use of social media and public participation in origination and dissemination of alerts and warnings. This includes research and testing in the areas of standardization, aggregation and analysis, behavioral response, best practices, and privacy.

Interoperable Emergency Communications

FRG.07 – Emergency Medical Services (EMS) Color Requirements for Compressed Video: Gather EMS color requirements for compressed video. More than in other public safety applications, video used for EMS applications must retain color truth throughout the video system. Any impairment of color information during the recording, transfer, and/or display of video could be life-threatening as the color of blood and skin is often used to make critical diagnoses. In particular, the transmission of video over mobile networks (e.g. from an

ambulance in route) is problematic because of the compression which must be applied to the video stream in order to transmit it over the limited available wireless bandwidth.

FRG.08 – Video Quality Assessment for Recognition Tasks: Perform a video quality assessment for recognition task-based video. Recognition task-based video includes any applications in which users are concerned with the ability to recognize areas of interest in the video stream to specified levels of discrimination. Subjective experiments must be performed to develop accurate objective measurements for video quality assessment. The recognition can be either by human viewers or through automatic recognition systems. The recognition tasks could consist of fire detection, people counting, human monitoring, gait recognition, objective resolution measurements, object recognition, detecting objects and vehicles, characters, parking systems, license plate recognition, facial recognition, etc. The purpose is to advance the field of video quality assessment through the collaborative development of performance specifications and standards for task-based video.

FRG.09 – Simulation Testbed for Transport Components' Performance Analysis in a Video System: Design a simulation testbed for analyzing the transport components' performance in a video system. The testbed would be validated by using different types of cameras to identify the limits of camera use for streaming video (with or without compression) on a given network. The research result would be a web tool (or Application Programming Interface) that illustrates the use of a simulated testbed to define network bandwidth requirements for a video system.

FRG.10 – Conformance testing tools for Project 25 (P25) interfaces: Develop a commercially available conformance test tool for the P25 Common Air Interface (CAI). The tool needs to incorporate all of the P25 Compliance Assessment Program selected tests for the CAI including conventional and trunked operations for both subscriber units and base station/repeaters. The tool should incorporate a self-assessment capability to ensure proper operation, and should generate detailed reports.

Information Sharing

FRG.11 – Regional Information Sharing: Develops, evaluates, and establishes methodologies, processes, and systems for the integration of existing information sharing frameworks and technologies to enable collaboration at the local, tribal, state, and Federal levels. This includes capability gap identification, requirements gathering, prototyping, and the creation and establishment of best practices.

Infrastructure Protection and Disaster Management

IDD.01 – Concepts, methodologies, algorithms, and/or technologies for identifying, understanding, and mitigating all-hazard vulnerabilities of the 18 critical infrastructure sectors. Concepts, methodologies, and/or technologies for improving the preparedness and disaster management response capabilities for Federal, State, local, tribal governments, first responders and the private sector, to all-hazards events impacting the United States population, critical infrastructure, and the economy. Improved understanding of natural hazards and development of mitigation measures to protect against them.

IDD.02 – Advanced Materials: Renew the infrastructure of the present and construct the infrastructure of the future to be resistant to many hazards and have sustainable properties. Hazards include blast, projectiles, fire, earthquakes, wind, flooding, deterioration and aging, corrosion, and especially combinations of these design challenges. Sustainable properties include self-healing, self-diagnosing, self-reporting, generating or conserving energy, minimal drain on nonrenewable resources, conserving water, long life, and affordability.

IDD.03 – Blast & Projectile Analysis and Design of Protective Measures: Understanding the basic physics of blast effects on infrastructure that has not received extensive past testing and analysis (e.g., dams, levees, tunnels, bridges); improved understanding and modeling of blast effects on critical components of the infrastructure systems (e.g., bridge towers, cables, submerged infrastructure); and design of either protective measures to limit damage or expeditious means to shore up damaged infrastructure and protect against further loss of life.

IDD.04 – Resilient and Sustainable Infrastructure: Enhancing security, resilience, and recovery of the 18 critical infrastructure sectors for new and retrofit applications. Develop key critical infrastructure components that are affordable, highly transportable, and provide robust solutions during manmade and natural disruptions. Integrate infrastructure protection design with sustainable technologies and methodologies to reduce the consumption of energy, promote clean water, decrease pollutant emissions, and aim at resource conservation over the life of the project. It should use high-performance green materials that are self-monitoring, are self-healing, and stand the test of time. It should resist blast, earthquake, floods, and wind. Developing infrastructure that is sustainable means thinking differently about how we build, what we build, and whether we build at all. It means designing and maintaining infrastructures that are both highly efficient and all-hazard–resistant.

IDD.05 – Advanced Surveillance and Monitoring: Integration of multiple types of sensing technologies and intelligent algorithms to allow for more efficient acquisition and interpretation of data, including identification and tracking in crowded environments and enhanced detection and reporting of anomalous activities.

IDD.06 – Modeling, Simulation & Analysis (MSA) and Decision Support Systems (DSS): Concepts, techniques, methodologies, algorithms, and innovative tools and applications to significantly enhance the quality of system analysis and reduce the time/cost of conducting system analyses. Modeling tools for a wide range of decision makers, from local law enforcement to governors to the White House, to evaluate alternative policies and actions to deal with emergencies and anticipate cascading effects across interdependent systems. Tools for real-time decision support in emergencies capable of integrating and assimilating multiple types of information, processing that information, and presenting it in a manner useful to decision makers. Visualization and Analytics: Mathematical methods, computational algorithms, and hardware architectures for discovering, comprehending, and manipulating diverse, diffuse data or information and applying the resulting knowledge to assess threats and consequences, anticipate terrorist incidents and natural or manmade catastrophic events, and guide response and recovery activities. Capabilities sought include the following:

- ✓ (1) Dynamic, on-Demand, and Real-time Information Processing and Visualization;

- ✓ (2) Hypothesis-driven and Game-based Analysis;
- ✓ (3) Visualization of Structured, Unstructured, and Streaming Data;
- ✓ (4) Scalable Filtering and Dissemination;
- ✓ (5) Simulation and Modeling for Threat and Disaster Mitigation;
- ✓ (6) Mobile, Light-weight Information Analytics and Sharing;
- ✓ (7) Discrete Mathematics and Data-intensive Computing Foundations of Data Analytics;
- ✓ (8) Precision Information Environments for Decision-making.

IDD.07 – Cyber-physical Systems Security: Cyber-physical systems (CPS), which are emerging trend across the globe, are characterized by tight coupling, coordination, and interconnections among sensing, communications, computational, and physical resources. CPS are exhibited in many application areas, including industrial control systems, and are prevalent in almost every critical infrastructure sector, including water, gas, electricity, transportation, chemical, and healthcare. Such interconnections form a complex system of systems. It is envisioned that the complexity of the cyber-physical systems of the future will far exceed that of today, which poses several research challenges related to resiliency, vulnerability, threat, and recovery assessment issues. Models, theories, methods, and tools to address the security of cyber-physical systems taking into account the cyber and physical components of a system in an integrated and unified way and realizing the discrete and continuous aspects of the system.

IDD.08 – Integrated Incident Management: components and systems to improve public, emergency management and first responder situational awareness, capability, and safety. Increased situational awareness to manage available and anticipated human and material resources, transportation capabilities, and the need for timely information to support critical decisions involving rapidly shifting priorities; geospatial data to create a seamless system among Federal, State, and local and tribal first responders; and established virtual continuity of operations (COOP) capabilities to improve incident management when key infrastructures and facilities are unavailable. Cost effective enhanced analytical capabilities for improving data analysis, situational awareness and actionable information sharing across Federal, State, and local and tribal public safety organizations.

- **IDD.08.1** – Information Sharing: Supports improved situational awareness and decision making across Federal, state, local, tribal and territorial public safety organizations, as well as non governmental agencies, private sector partners organizations and the public and communities. Seeks concepts, prototypes and technologies that improve the capability to collect, process, analyze, visualize, share, and protect information across the Homeland Security Enterprise.

- **IDD.08.2** – Geospatial and Remote Sensing: Geospatial technologies that enhance situational awareness for the protection of critical infrastructure and improved management of incidents at Federal, State, and local and tribal levels. Image processing and spatial analytical techniques that exploit remote sensing measurements to improve detection of specific phenomena of interest to first responders. Web services that provide improved analytical capability using cloud

computing or distributive architectures to provide critical products to all levels of incident command.

IDD.09 – First Responders: Advances to improve protection of or enhance performance of responders as they carry out life-saving tasks. Technologies that will fully enable emergency managers and first responders to effectively cope with multi-hazard emergencies—technologies such as advanced materials for protective clothing that report on the health of the first responder; decision support systems that provide real-time logistical tracking and management of emergency supplies, equipment, and personnel; advanced 3-D tracking technologies; an integrated and simulation-based incident planning and response capability to analyze all-hazard disaster response and recovery operations, tactics, techniques, plans, and procedures for use in a real-time environment for simulation-based training. Use industrial standards to develop advanced algorithms, tools, and infrastructures for sensor data fusion and visualization for improved situational awareness and emergency response.

IDD.10 – Physics and Mitigation of Natural Hazards: Improved capabilities to anticipate, prepare for, and/or mitigate the impact of catastrophic physical phenomena. Better understand the physics that drive the internal processes and severity of natural hazards to develop innovative, effective protective measures that reduce damage from natural hazards, minimize their impact on critical infrastructure, and more quickly recover from them. Example hazards include hurricanes and the heat engine processes that control their intensity and resulting storm surge; solar storms resulting in geomagnetic impacts on earth; high winds, erosion, and flooding; wildfires; and processes driven by high winds and drought, protective design and rapidly deployable protective measures; and earthquakes, including an ability to interpret signals from the earth to estimate the timing, location, and severity of an earthquake.

Human Factors/Behavioral Sciences

HFD.01 – Human Factors/Behavioral Sciences applies the social and behavioral sciences to improve detection, analysis, and understanding of threats posed by individuals, groups, and radical movements; develops novel technologies and tools to improve the recognition of individuals; supports the preparedness, response, and recovery of communities impacted by catastrophic events including support for first responders; and advances national security by integrating human factors and public perceptions data into homeland security technologies.

HFD.02 – Behavior-based methods, models and technologies to enhance community resilience in the face of human- or nature-caused catastrophes through such means as better understanding of risk perception, improved risk communication by emergency responders and public officials, programs of pre-event education and training and applied theoretical and empirical research into the properties of resilient social networks and communities, including more effective ways of mapping and linking emergency response, longer term recovery teams and other organizations within and across the public, faith-based, NGO and private commercial sectors.

HFD.03 – Research into metrics related to resilience, including the creation of validated metrics measuring the psychosocial impact of large-scale disasters and catastrophes on affected

individuals and communities and measures of the effectiveness of societal and community resilience efforts across physical, economic, social, psychological and cultural dimensions.

HFD.04 – Research and technology to improve knowledge and skill acquisition and human and team performance in the context of user interfaces, including research designed to achieve a better understanding of the range of fundamental human processes (physiological, neurological, behavioral, physical, perceptual, and cognitive) that affect individual human and team performance; as well as research into the development of tools and processes that support analysis of human performance requirements, identification of human performance risks, and performance of user-centered design and test and evaluation.

HFD.05 – Research into terrorist motivations, intent, recruitment, mobilization, and operations in order to develop a framework for assessing threats to the homeland, including the use of IEDs.

HFD.06 – Tools and technologies to determine when radical groups are likely to engage in violence, and what ideological, organizational, and contextual factors may influence violent action.

HFD.07 – Methods for non-invasively identifying deceptive and suspicious behavior within a time constrained, low-base rate, screening environment, and methods for identifying interactive strategies optimal for eliciting disguise-resistant indicators of deceptive and suspicious behavior, including technologies that automate or aid in such identification.

HFD.08 – Protocols and technologies to minimize insider threats and to identify insider threat behavior when it occurs, especially in settings like transportation security or at a border.

HFD.09 – Improvements in biometrics, including real-time positive verification of individual identity using multiple biometrics; mobile biometrics screening capabilities, high-fidelity tem print capture, remote biometrics and the development of standards and test/evaluation protocols.

HSARPA/Innovation

HID.01 – Apex was recently launched to address specific & urgent S&T needs for the Department. Apex projects are focused on enhancing DHS Operational Component partner capabilities to secure the homeland. Apex projects:

- Rapidly develop and deliver analyses and innovative technologies solutions to DHS Components
- Are closely collaborated with the DHS Components throughout planning and execution
- Use rigor to define the problem, needs and capabilities to enhance DHS Component's mission
- Develop a complete solution that includes systems analysis
- Deliver technologies that integrate in to the DHS Component's operations
- Use a multidisciplinary team to leverage the breadth of S&T knowledge
- Are 24 months from project inception through operational testing

HID.02 – The current Apex project has one technology goal: Implement new technologies to upgrade and increase the DHS Component's ability to protect people and things. This includes emerging technologies that are lightweight, efficient, modular, and easily transportable. The technology solutions proposed must integrate with existing technologies used by the DHS Component, and be acceptable to the DHS Component.

Topical Areas of strategic interest include:

HID.03 -- Information Resources: Develop, test, evaluate information systems and analytical tools to enhance preparation, facilitate decision making, and improve incident response capabilities. Develop, test, and evaluate software tools to more efficiently exploit intelligence and surveillance data.

HID.04 -- Communications, Surveillance and Reconnaissance: Develop, test, and evaluate surveillance and communication systems/sensors that enhance the protection of personnel and mitigate threats.

HID.05 -- Individual Protection: Develop, test, and evaluate enhancements to the protection of personnel during blast and ballistic events. Develop and test technologies that improve the performance of body armor by reducing weight and optimizing material performance.

HID.06 -- Mobile Security: Enhance personnel protection during mobility (vehicular, etc.) operations.

8. SUBMISSION PROCESS, CLASSIFIED INFORMATION

LRBAA Submission Website

All LRBAA submissions, including White Papers and Full Proposals, must be made through the S&T BAA website: https://baa2.st.dhs.gov.

To begin the registration process, go to https://baa2.st.dhs.gov and select the *Proposal Submission* link from the side menu. From there, select the *Register* link. You will need to know your company Tax Identification Number to complete the registration. Submissions will not be accepted from unregistered organizations. Once registered, log into the system and select BAA 11-03 to begin making submissions. You may contact technical support for the website at dhsbaa@reisys.com or (703) 480-7676.

Only unclassified White Papers and Full Proposals may be submitted via the LRBAA website. For instructions on how to submit classified information, please refer to the instructions in this section below.

Oral presentations are not permitted at any point during the LRBAA 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 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.

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.

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. 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.

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 Documents

Classified White Papers and Full Proposals cannot be transmitted via the LRBAA website. However, Offerors must still first register online following the registration instructions, log in, and initiate a White Paper submission. Offerors shall print out the completed cover sheet and attach it to the classified submittal. Offerors shall 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. 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). Offerors may view the NISPOM document online at http://www.dss.mil/isec/nispom.htm. 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.

Classified submissions can be emailed to: shane.davis.@dhs.sgov.gov

Please send an unclassified alert email to shane.davis@dhs.sgov.gov , LRBAA.Admin@hq.dhs.gov, and LRBAA.OPO@hq.dhs.gov **before** emailing classified information.

9. CONTENT AND FORMAT

Submissions that do not comply with these instructions will be rejected without further review.

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.
- ✓ 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. Limitations within sections of the technical proposal are indicated in the individual descriptions shown below. 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, and resumes 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 LRBAA 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: The cover sheet is automatically generated during the submission of the White Paper to the LRBAA website. *This is not the same as the Offeror's cover page.*

- Cover Page: The cover page shall include the words "Technical Proposal" and the following:

  1) BAA number 11-03;
  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);
  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: This is an 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: Summary of the proposed research and the benefits expected from this investment.

- Landscape Assessment or Brief Literature Review: Explain why your proposal is different and superior to similar solutions already available or to the efforts of others who have been researching similar issues.

- Proposed Use for DHS S&T: A detailed explanation of how the proposed product(s) supports the targeted end user (e.g., the first responder community) in an operational context. Include quantitative specifications for how the products will improve operational performance.

- Technical Concept: A description of the technical concept, including anticipated risks and approaches to mitigate the risks. Describe the basic scientific or technical concepts that will be used in each component or subsystem comprising your proposed solution to the problem

described above. What particular scientific, technical or engineering issues need to be addressed and resolved to demonstrate feasibility? What is unique about your solution and what advantages might it afford compared to alternative approaches that others have taken? What has been the extent of the principal investigator's past experience in, and qualifications or educational background for, developing the technologies in your proposal?

- Operational Concept: A description of the operational concept used in the proposed technical solution to accomplish the objectives. Explain how the performance of your proposed solution can be expected to meet or exceed and be measured against each of the specific technical attributes and/or performance enhancements. What are the key scientific, technical, or engineering challenges and the timing for each that must be met in order to successfully complete this project? Describe all required material and information, which must be provided by the Government to support the proposed work.

- Operational Utility Assessment Plan: A detailed plan for demonstrating and evaluating the operational effectiveness of the Offeror's products in exercises, including evaluation metrics. Explain your view of the requirements gap to be filled, what capability will be provided upon successful completion of the proposed effort, and what are the technical risks associated with successful maturation of the proposed effort to achieve operational utility. Explain your concept of how you will develop and demonstrate a system or system component. Identify and explain the critical path technologies or key technical challenges you will face when building this system or component and your plans for meeting these challenges. Explain how you will demonstrate the system or component performance relative to the performance or enhancement goals described in the proposal.

- Statement of Work: A Statement of Work (SOW) and a Work Breakdown Structure (WBS) that clearly detail the scope and objectives of the effort, the technical approach, and the performance goals. The SOW and WBS will be used in the development of any final award, so the proposal must include a stand-alone SOW and a stand-alone WBS without any proprietary restrictions. The WBS must include a detailed listing of the technical tasks/subtasks in hierarchical fashion for the tasks required to accomplish the effort. The WBS format must be complete to at least WBS level three. Each task in the SOW shall describe the work to be carried out, the end result of the task, the time allocated, the organization performing the task, the predecessor tasks, the performance goals of the task, and the resources (labor, materials, and services) required. The resources shall be costed to provide a baseline budgeted cost for the applicable task. The SOW shall be at a level sufficient to define the nature of the work to be carried out, measure progress, and demonstrate the relationship of the tasks to one another.

- Project Schedule and Milestones: A summary of the schedule of events and milestones. If applicable, identify the critical path.

- Deliverables: A detailed list and description of all deliverables and data deliverables the Offeror proposes to provide to the Government, the schedule for delivery, and acceptance criteria. The deliverables information must be a separate section in the Offeror's proposal and begin on a new page. Proposals must include a severable self-standing detailed list

and description of all deliverables without any proprietary restrictions, which can be used to make award.

- Qualifications: A discussion of the Offeror's previous accomplishments and work in this area, or closely related area, and the qualifications of the investigators. If the proposal involves development or testing scientific and/or engineering concepts, the principal investigators must demonstrate education and/or managerial expertise in these fields. Key personnel resumes must be attached to the proposal and do not count toward the page limitations.

- Detailed Risk Mitigation Plan: Discuss in detail the technical, cost, and schedule risk(s) involved with the project and how each risk will be mitigated.

- Management Approach: A discussion of the overall approach to the management of the effort, including brief discussions of the total organization, use of personnel, project, function, and subcontractor relationships, government research interfaces, and planning, scheduling and control practice. Identify which personnel and subcontractors (if any) will be involved. Include a description of the facilities that are required for the proposed effort with a description of any Government-Furnished Equipment/Hardware/ Software/ Information required, by version and/or configuration.

- Small Business Considerations: Full Proposals that exceed $650,000, submitted by all but small business concerns, must include a Small Business Subcontracting Plan in accordance with FAR 52.219-9. The Small Business Subcontracting Plan is included in the 40 page limit. Regardless of the proposed dollar value, all Offerors shall indicate their business size status and list all subcontractors and their business size statuses. All LRBAA Offerors are encouraged to offer subcontracting opportunities to small businesses to the maximum extent practicable.

- Include a statement specifying compliance with FAR Clause 52.222-54 Employment Eligibility Verification.

- Assertion of Data Rights: Include here a summary of any assertions of rights to any technical data or computer software that will be developed or delivered under any resultant award. This includes any assertions to pre-existing results, prototypes, or systems supporting or necessary for the use of the research, results, or prototype. Any rights asserted in other parts of the proposal that would impact the rights in this section must be cross-referenced. If less than unlimited rights in any data delivered under the resultant award are asserted, the Offeror must explain how these rights in the data will affect its ability to deliver research data, subsystems, and toolkits for integration as set forth below. Additionally, the Offeror must explain how the program goals are achievable in light of these proprietary and/or restrictive limitations. If there are no claims of proprietary rights in pre-existing data, this section shall consist of a statement to that effect.

Proposals submitted in response to this Announcement shall identify all technical data or computer software that the Offeror asserts will be furnished to the Government with restrictions on access, use, modification, reproduction, release, performance, display, or disclosure. Offerors' pre-award identification shall be submitted as an attachment to its offer and shall contain the following information:

(1) *Statement of Assertion.* Include the following statement: "The Offeror asserts for itself, or the persons identified below, that the Government's rights to access, use, modify, reproduce, release, perform, display, or disclose only the following technical data or computer software should be restricted."

(2) *Identification of the technical data or computer software to be furnished with restrictions.* For technical data (other than computer software documentation) pertaining to items, components, or processes developed at private expense, identify both the deliverable technical data and each such item, component, or process as specifically as possible (e.g., by referencing specific sections of the proposal or specific technology or components). For computer software or computer software documentation, identify the software or documentation by specific name or module or item number.

(3) *Detailed description of the asserted restrictions.* For each of the technical data or computer software identified above in paragraph (2), identify the following information:

(i) Asserted rights. Identify the asserted rights for the technical data or computer software.

(ii) Copies of negotiated, commercial, and other non-standard licenses. Offeror shall attach to its offer for each listed item copies of all proposed negotiated license(s), Offeror's standard commercial license(s), and any other asserted restrictions other than Government purpose rights; limited rights; restricted rights; rights under prior Government contracts, including SBIR data rights for which the protection period has not expired; or Government's minimum rights.

(iii) Specific basis for assertion. Identify the specific basis for the assertion. For example:

- Development at private expense, either exclusively or partially. For technical data, development refers to development of the item, component, or process to which the data pertains. For computer software, development refers to the development of the software. Indicate whether development was accomplished exclusively or partially at private expense.
- Rights under a prior government contract, including SBIR data rights for which the protection period has not expired.
- Standard commercial license customarily provided to the public.

- Negotiated license rights.

(iv) Entity asserting restrictions. Identify the corporation, partnership, individual, or other person, as appropriate, asserting the restrictions.

(4) *Previously delivered technical data or computer software.* The Offeror shall identify the technical data or computer software that are identical or substantially similar to technical data or computer software that the Offeror has produced for, delivered to, or is obligated to deliver to the Government under any contract or subcontract. The Offeror need not identify commercial technical data or computer software delivered subject to a standard commercial license.

(5) *Estimated Cost of Development.* The estimated cost of development for that technical data or computer software to be delivered with less than Unlimited Rights.

(6) *Supplemental information.* When requested by the Contracting Officer, the Offeror shall provide sufficient information to enable the Contracting Officer to evaluate the Offeror's assertions. Sufficient information must include, but is not limited to, the following:

- The contract number under which the data or software were produced;
- The contract number under which, and the name and address of the organization to whom, the data or software were most recently delivered or will be delivered; and
- Identification of the expiration date for any limitations on the Government's rights to access, use, modify, reproduce, release, perform, display, or disclose the data or software, when applicable.

(7) *Ineligibility for award.* Failure to submit or complete the identifications and assertions required by this provision may render the Offeror ineligible for award.

Please Note: The section entitled "Assertion of Data Rights," must be severable, i.e. it must start on a new page. It is anticipated that the proposed Assertion of Data Rights section will be incorporated as an attachment to the resultant award instrument. Proposals must include a severable self-standing Assertion of Data Rights section without any proprietary restrictions, which can be used to make the contract or agreement award.

Volume 2: Cost Proposal

- Cover Sheet: The cover sheet is automatically generated during the submission of the White Paper to the LRBAA 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 11-03;
    2) Title of proposal;
    3) Topical area and reference code;
    4) Identity of prime Offeror, including name and address, and complete list of subcontractors, including names and addresses, if applicable;
    5) Technical contact (name, address, phone/fax, electronic mail address);
    6) Administrative/business contact (name, address, phone/fax, electronic mail address);
    7) Duration of effort (separately price out the basic effort and any options);
    8) DUNS number and CAGE code;
    9) Statement on whether or not the Offeror has been audited by a Government organization (Defense Contract Audit Agency, Office of Naval Research, etc.), and if the Offeror has a Government-approved accounting system;
    10) DCAA point of contact (name, telephone number, and email address);

Cost Proposal Part 1

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

- Direct Labor: Individual labor category or person, with associated labor hours and **unburdened** direct labor rates.

- Indirect Costs: Fringe Benefits, Overhead, G&A, COM, etc. (Must show base amount and rate).

- (If applicable and available) Forward Pricing Rate Agreement (FPRA) or Defense Contract Audit Agency (DCAA) approved or recommended rates. Identify if there are outstanding CAS violations.

- 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

The 2011 LRBAA will remain open until December 31, 2011, 11:59 PM Eastern, during which time White Papers and Full Proposals may be submitted in accordance with the instructions described in this document. No submissions will be accepted after the closing date.

Evaluations and awards will occur on a "rolling selection" basis. Generally, evaluations will 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 and/or subject to availability of funds. Full Proposals submitted should cite a validity timeframe of 180 days.

Offerors should take note that, as of this document's writing, the federal government is operating under a Continuing Resolution. The Continuing Resolution may continue beyond March 2011. It funds continuing governmental projects and activities that were conducted in fiscal year 2010, for which appropriations, funds, or other authority were previously available. The Continuing Resolution prohibits the initiation of new programs or expanding the scopes of existing programs, projects, or activities, referred to as "New Starts." Depending on the duration of the Continuing Resolution, awards based on this LRBAA may be affected; the Government may opt to defer awards, make awards subject to the availability of funds, or take other measures.

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 LRBAA submissions. Contractors will provide administrative support, principally including technical advice to Government employees, to the Source Selection Evaluation Boards. Submissions will be evaluated only by authorized Government employees; only Government employees will sit on Source Selection Evaluation Boards. In submitting a White Paper of Full Proposal, Offerors consent to allow contractor access to submissions. All contractors who provide support services to S&T for LRBAA activities have signed general non-disclosure agreements and, where applicable, organizational conflict of interest statements.

12. EVALUATION INFORMATION

Evaluation Factors and Subfactors

White Papers and 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. The Offeror's understanding of the project's risks, and how these risks have been identified and how they are being addressed, as well as how the proposed solution compares to similar work performed.

B. Mission relevance.

Extent to which the work proposed applies to one of DHS's operational security environments and the needs of S&T as described beginning on page 6.

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, 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 negotiation and possible award based on evaluation using the factors and subfactors described above, through a scientific or peer review process, as described in FAR 35.016(d) and (e).

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 http://www.ccr.gov/.

- Certifications: In accordance with FAR 4.1201, prospective Offerors for contracts, and other transaction agreements involving prototypes, shall complete the Online Representations and Certifications Application (ORCA) at http://orca.bpn.gov. Offerors shall make mention of its ORCA completion in its proposal, and provide its "Certification Validity" period. Successful Offerors will be provided additional information with regards to certification for grants, cooperative agreements, or other transaction agreements (other than for prototypes) proposals.

- 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 regarding 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 or other transactions agreements 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, via the *Awardee Portal* section of https://baa2.st.dhs.gov, to the program manager within one week after the last day of each month. These reports must describe the previous calendar month's activity, technical progress achieved against goals, difficulties encountered, recovery plans (if needed), explicit plans for the next calendar month, and financial expenditures (including expenditures during the past calendar month period plus cumulative expenditures, and projected expenditures for the coming calendar month).

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.

Security Classification

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 information classified to the level of (SECRET or TOP SECRET). For personnel, a minimum of a (SECRET or TOP SECRET) clearance would be required. Any contractor facilities used in support of such a contract would require (SECRET or TOP SECRET) facility clearances and have the capability to store material classified up to and including (SECRET or TOP SECRET). A DD Form 254 would be required prior to access or production of any classified information. Additionally, the contractor is required to safeguard the information labeled as proprietary.

Any security concerns must be addressed to:

Shane Davis
Science and Technology Directorate
Department of Homeland Security
Unclassified email: shane.davis@hq.dhs.gov

Classified email: shane.davis@dhs.sgov.gov
Office: 202-254-5749
Fax: 202-254-5783

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. Interim meetings are likely, but these will be accomplished via video telephone conferences, telephone conferences, or via web-based collaboration tools.

Information for White Paper and Full Proposal Respondents

This LRBAA is for planning purposes only and must not be construed as an obligation on the part of the Government to acquire any products or services. No entitlement to payment of direct or indirect costs or charges by the government will arise as a result of submission of responses to this LRBAA and the Government's use of such information. Respondents to this LRBAA may be requested to provide additional information based on their submittals. Unnecessarily elaborate responses containing extensive marketing materials are considered unresponsive to this LRBAA.

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 White Paper Format
White Paper Must Not Exceed 5 Pages Total.
DHS S&T LRBAA 11-03 White Paper Format for Calendar Year 2011

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
List of Tasks and Schedule (From Award Date)
Task 1: (Start to Month ___) Task 2: (Month ___ to ___) Task N: (Month ___ to ___) **Total Duration of Project:**
Estimated Cost of Each Task/Total Project Cost
Breakdown of Costs by Tasks: Task 1 Cost: Task 2 Cost: Task N Cost: **Total Cost:**
Description of Deliverable(s) and Schedule of Delivery
Deliverable 1: ____ (Award Date + ___months) Deliverable 2: ____ (Award Date + ___ months) Deliverable N:____ (Award Date +___ months)
Major Milestone(s) for Task and Phase Completion as well as Follow-On Work
Task Milestone(s): *[Criteria for completion of particular Task(s)]* (Award Date + ___ months) Phase Milestone(s): *[Criteria for completion of particular Phase(s)]* (Award Date + months)
Offeror's capabilities, related experience, and past performance, including the qualifications, capabilities, and experience of the proposed principal investigator and personnel
Subcontracting Commitment
Comments

NOTE: Resumes are not requested for White Paper submissions; qualifications must be included.