



**Department of Homeland Security (DHS)
Science and Technology (S&T) Directorate**

**Long Range Broad Agency Announcement (LRBAA) 18-01
AMENDMENT 4**

LRBAA 18-01 TABLE OF CONTENTS

SECTION	LINKED TITLE
1	<u>LRBAA INTRODUCTION</u>
2	<u>PROCESS OVERVIEW</u>
3	<u>ELIGIBILITY</u>
4	<u>RESEARCH TOPICS</u>
5	<u>PROCESS DETAIL</u>
6	<u>TERMS AND CONDITIONS</u>
7	<u>CONTACTS</u>
8	<u>LRBAA ATTACHMENTS</u>

The Department of Homeland Security (DHS), Science and Technology (S&T) Directorate announces a modernized Long Range Broad Agency Announcement (LRBAA) featuring improved communications, transparent needs, submission options, and a faster response to your submissions. The LRBAA's purpose is to fund scientific and technical projects across a spectrum of science and engineering disciplines that significantly improves or increases a capability to the Department's operational environment and the Homeland Security Enterprise.

DHS S&T is interested in receiving research concept materials that meet one of the following three types of research areas:

- Type I (New Technologies): Scientific study and experimentation directed towards advancing unique state-of-the-art research, technology development, and demonstration. Emphasis for this type classification is on research and development, with technology demonstration in an operational environment;
- Type II: (Unique Prototype Technologies) Includes the development of prototypes that require a proof of concept, including technology demonstrations in an operational environment; and
- Type III: (Advance State of the Art Technology Improvements) Increases scientific discovery or improvements in technology, materials, processes, methods, devices or techniques. Includes technology demonstration in an operational environment.

LRBAA awards may consist of basic and applied research contracts, grants, cooperative agreements and/or other transactions agreements, to include technology development and demonstration. This LRBAA will NOT pursue the following solutions:

- Technical, engineering, or other types of support services, inclusive of "contracting"- type services;
- Evaluation of another contractor's performance/program;
- Research consortia, association, partnership or a combination, as of businesses or investors, for the purpose of engaging in a joint research and development venture for a particular purpose;
- Mature products; or
- Development of a specific system or hardware solution.

The DHS S&T LRBAA 18-01 is a five (5) year announcement and will remain open until June 3, 2023, 11:59PM, Eastern Daylight Time (EDT). This announcement may also contain topics with a limited open submission period. Industry Engagement materials are due by June 3, 2023, 11:59PM, EDT or as indicated in this announcement in order to be further considered for an invitation to participate in the LRBAA's Phase I-Virtual Pitch and Phase II-Written Proposal. Please be advised that the response dates associated with Phase I-Virtual Pitch and Phase II- Written Proposal will be the date specified in the notification letter provided to you and not the LRBAA completion date of June 3, 2023, 11:59PM, EDT, referenced above.

Technical and cost proposal (or any other material) development costs will not be reimbursed. Technical and cost proposals (or any other material) submitted in response to this LRBA will not be returned. However, depending on the markings on the materials, DHS S&T will adhere to FAR policy on handling source selection and proprietary information. It is the policy of DHS S&T to treat all materials as proprietary information and to disclose their contents only for the purposes of evaluation. **Please note only unclassified Materials may be submitted via the LRBA website. Classified information must not be transmitted via the LRBA website.**

Awards under the LRBA will depend on the quality of proposals received and the availability of funds. The Government reserves the right to select all, some, one or none of the invited proposals received, and/or to accept proposals in their entirety or to select only portions of proposals for award. The Government reserves the right to award without exchanges or discussions. Award decisions will result from a scientific and best value determination as further detailed in this announcement. Awards may take the form of Federal Acquisition Regulation (FAR) –based contracts; or grants, cooperative agreements, Other Transaction Agreements (OTA), or interagency agreements to appropriate parties should the situation warrant.

The applicable laws and regulations governing a particular award will depend on the selected award type as referenced in the previous paragraph. DHS S&T will also facilitate access to laboratory and operationally relevant test and evaluation facilities, where reasonably available. In the event that an Offeror or Offeror's subcontractor is a Federally Funded Research and Development Centers (FFRDC), Department of Energy National Laboratory, or other federal entity, DHS S&T will work with the appropriate sponsoring agency to issue an interagency agreement pursuant to the Economy Act (31 USC 1531) or other appropriate authority. In many cases, other elements of the U.S. Government are pursuing related technologies. In such cases, S&T will leverage those technology development efforts wherever it is practicable and efficient to do so.

DHS S&T LRBA Submission Portal Website: <https://baa2.st.dhs.gov>

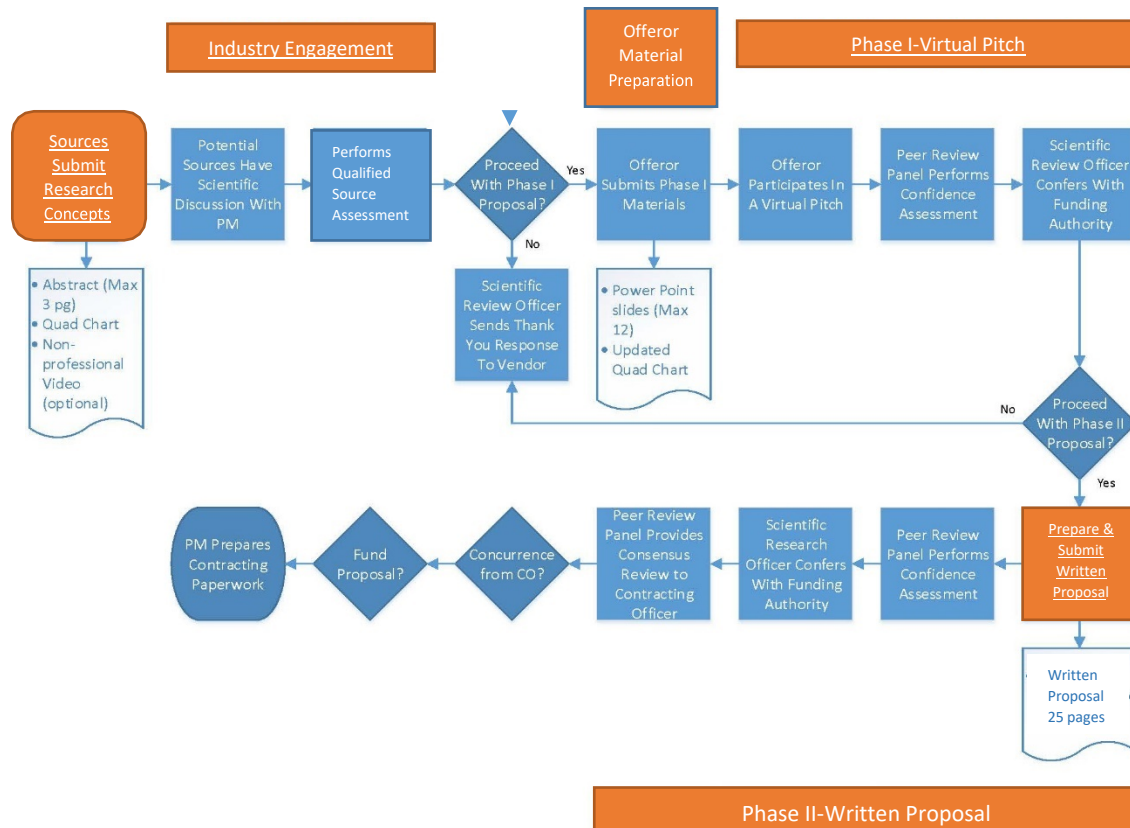
The LRBA begins with an Industry Engagement period. During the Industry Engagement period Project Managers (PMs) engage with interested sources in order to identify a broad range of qualified sources in the scientific and industrial community. Qualified sources may be invited by a S&T Scientific Review Officer to participate in the two-phase proposal process consisting of a Phase I-Virtual Pitch and a Phase II-Written Proposal. Submission requirements and details are further outlined in this announcement.

A Phase I-Virtual Pitch proposal will not be accepted from any Source that has not been invited to submit. Offerors that submit to and participate in the Phase I Proposal-Virtual Pitch may be invited by a Scientific Review Officer to participate in the Phase II-Written Proposal. Unique proposals submitted to the Phase I-Virtual Pitch that meet high priority technology requirements but exceed available funding may not be immediately invited to submit a Phase II-Written Proposal. Phase II-Written Proposals will not be accepted from an Offeror that has not been invited to submit.

The below chart maps the DHS S&T LRBA process from the initial submission to award. The three primary submission and evaluation processes are indicated in orange and contain hyperlinks to submission, evaluation and administrative details. (Also see Section 5)

Long Range Broad Agency Announcement Process Flow Chart

Learn More-Click on Orange Boxes



Submission and Evaluation Timeframes

The following timeframes have been established for the LRBA submission and evaluation process. Sources and Offerors should allow 2-5 days at the end of each assessment or evaluation period for administrative processing and notification. In some instances, the assessment or evaluation period may be extended due to the availability of subject matter personnel required for the Peer Review Panel. DHS S&T Program Managers will work closely with sources and offerors to keep them informed of their submission and assessment status.

Process	Timeframe
Industry Engagement Assessment	Response and follow-up by S&T within 10 Days
Part I-Virtual Pitch presentation material	Must be submitted to the LRBA Submission Portal within 14 Days of written notification
Part I-Virtual Pitch and Evaluation	Scheduled within 21 Days of the presentation material's due date
Part II-Written Proposal	Must be submitted to the LRBA Submission Portal within 45 days of written notification
Part II-Written Proposal Evaluation	Completed by S&T within 21 days of the written proposals due date

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

All responsible sources are eligible to submit Industry Engagement materials under this LRBA.

Foreign or foreign-owned sources 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. Potential sources may include independent organizations, single entities, or teams from private sector organizations, Government laboratories, airport authorities, FFRDCs, and academic institutions. FFRDCs, including the Department of Energy National Laboratories and Centers, are eligible to respond to this LRBA individually or as team members with eligible principal sources, as long as they are permitted to respond to such announcements under their applicable sponsoring agreements.

DHS S&T particularly encourages submissions from small businesses. However, no set aside of any kind will be made. 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 participate in the process and to join other entities as team members.

Protecting our nation can be complex – from rapidly evolving threats to longer-term efforts that require our attention. To fully understand the needs of our operational components, DHS S&T and Components routinely identify priority needs that require R&D solutions. The current six key mission areas are:

Securing Aviation
Securing Borders
Preventing Terrorism

Protecting from Terrorist Attacks
Securing Cyberspace
Managing Incidents

These priority needs drive DHS's R&D investments. DHS S&T and Components look for the following types of solutions:

1. Over the horizon, future innovations that will transform the way homeland security operators accomplish their missions.
2. Near-term capabilities that will solve current operational challenges and meet the Department's R&D needs.
3. New applications of technologies to respond to emerging threats to the homeland.

For more information about how DHS compiles these needs, visit our website at <https://www.dhs.gov/science-and-technology/ipt> and <https://www.dhs.gov/publication/stfrg-project-responder-5-report> to download our annual Integrated Product Team and Project Responder reports describing the process and priority capability needs in further detail.

(Note: Additional details for each topic listed below can be found on the DHS S&T LRBA Submission Portal located at <https://baa2.st.dhs.gov/>)

SECURING AVIATION (SEC AVN)

The aviation security environment presents a constant demand to detect evolving threats while moving passengers, baggage, and cargo safely and quickly through checkpoints and promoting a positive passenger experience. The end goal is to provide non-invasive security screening at our nation's airports while preventing terrorist attacks and ensuring speedy and lawful trade and travel.

Priority R&D needs and topics for securing aviation are:

High-Throughput Cargo Screening (01)

Cost-effective Electronic Imaging for Bulk Air Cargo (02)

Passenger Identification and Vetting (03)

Rapid Detection and Alarming of Explosives (04)

SEC AVN 04-01: Canine R&D Structure and Function

TOPIC DESCRIPTION:

Canine R&D Structure and Function, part of the program focusing on the more basic understanding of canine behavior, genetics, olfaction, and cognition of this detector to improve operational efficiencies and training methods.

TOPIC RESEARCH SOUGHT: Type I

TRL SOUGHT: 4

TRL at CONCLUSION: 7

END OBJECTIVE:

Tools, techniques, and knowledge to better understand, train, and utilize the detection canine, and improve proficiency of the DHS/Homeland Security Enterprise (HSE) detection canine teams.

SEC AVN 04-02: Development and Testing of Canine Training Aids

TOPIC DESCRIPTION:

Development and Testing of Canine Training Aids, specifically targeting the creation of low cost, non-hazardous emerging threat and conventional explosive training aids, with state-of-the-art laboratory technology for odor validation to the level of canine detection. The program is also interested in odor generalization analysis studies to reduce requisite numbers of trained odors.

TOPIC RESEARCH SOUGHT: Type II

TRL SOUGHT: 4

TRL at CONCLUSION: 7

END OBJECTIVE:

S&T goals are to provide our customer base - TSA and the Homeland Security Enterprise (HSE) - with the tools, techniques, and knowledge to better understand, train, and utilize the detection canine and improve proficiency of the DHS/HSE detection canine teams. Provide an enduring research and development capability to the Homeland Security Enterprise with a unique focal point and knowledge base for detection canines by establishing a scientifically rigorous, statistically significant approach for the detection canine community that is currently absent in the industry.

SEC AVN 04-03: Independent Operational Test and Evaluation for Technologies and Methodologies That Advance Detection Canine Performance

TOPIC DESCRIPTION:

Technologies and methodologies that advance detection canine performance in controlled and operational environments representative of the Homeland Security Enterprise at the federal, state, and local level and facilitate scientifically significant data capture through independent operational test and evaluation.

TOPIC RESEARCH SOUGHT: Type III

TRL SOUGHT: 5

TRL at CONCLUSION: 7

END OBJECTIVE:

S&T's goals are to provide our customer base - TSA and the Homeland Security Enterprise (HSE) - with the tools, techniques, and knowledge to better understand, train, and utilize the detection canine, and improve proficiency of the DHS/HSE detection canine teams. Provide an enduring research and development capability to the Homeland Security Enterprise with a unique focal point and knowledge base for detection canines by establishing a scientifically rigorous, statistically significant approach for the detection canine community that is currently absent in the industry.

SEC AVN 04-08: Enhanced Contact and Non-Contact Trace Explosives Sampling and Detection

TOPIC DESCRIPTION:

The primary objective of this LRBA is to develop enhanced contact and non-contact trace explosives sampling methods and prototypes that are seamlessly integrated with or integration-ready with currently deployed Explosives Trace Detectors (ETDs) and/or Next Generation ETDs. The non-contact sampling methods and prototypes are developed for use in cargo, checked baggage, and or checkpoint screening in aviation security environments.

Currently, contact sampling (by swabbing) in aviation security environments requires divestiture and has limited throughput and detection libraries. Improvements to contact trace sampling has the promise of the ability to detect more threats of interest. Non-contact sampling technologies of both vapor and particulates have the potential to overcome these limitations by:

- Enlarging total surface areas of the objects undergoing screening
- Minimizing operator errors during automatic or semi-automatic sampling processes
- Enhancing passenger experiences

To realize the full potential of contact and non-contact sampling, candidate technologies must address the following challenges:

- 1) Have high efficiencies in liberating, entraining, and collecting explosive traces in both vapor and particulates
- 2) Broaden amenability to variable surface types (e.g. plastics, muslin, ballistic nylon, and clothing) yet maintain high collection efficiencies across these surface types
- 3) Not causing damage to the surfaces undergoing screening
- 4) Not contaminating the areas surrounding the objects undergoing screening
- 5) Optimize collection efficiencies for objects with varying shapes and sizes
- 6) Have provisions for the prototypes to seamlessly integrate with currently deployed ETDs and/or Next Gen ETDs
- 7) Provide the ability to detect a broader range of threats than currently available by currently deployed ETDs (especially for contact sampling methods)

TOPIC RESEARCH SOUGHT: Type II

TRL SOUGHT: 5

TRL AT CONCLUSION: 7

END OBJECTIVE:

Enhanced contact and non-contact trace explosives sampling methods and prototypes that are seamlessly integrated with or integration-ready with currently deployed Explosives Trace Detectors (ETDs) and/or Next Generation ETDs. The methods and prototypes are expected to be developed and undergo Developmental Test and Evaluation at a Government laboratory. Upon successful completion of Developmental Testing and Evaluation (DT&E) phase(s), the method/prototype may be selected for advancement to Integration Test and Evaluation.

Distinguishing Threats from Non-threats on Passengers (05)

Efficient and Accurate Detection of Complex Threat Concealment on Passengers and Carried Property (06)

SECURING BORDERS (SEC BORD)

Our borders are vital economic gateways that account for trillions of dollars in trade and travel

each year. Border security presents complex challenges due to geographic locations, modes of transportation, trade and travel volume, and transnational criminal organizations. DHS works to secure our borders through the deployment of personnel, infrastructure, and technology—including sensors, radar, and aerial assets—and investments to modernize the ports of entry.

Priority R&D needs for border security are:

Cross-border Tunnel Detection, Surveillance, and Forensics (01)

Infrastructure Tunnel Surveillance (02)

Integrated and Improved Sensors, Systems, and Data (03)

SEC BORD 03-05: Air Based Technologies

TOPIC DESCRIPTION:

The Air Based Technologies (ABT) program advances manned and unmanned aircraft technology to improve the mission capability of the DHS operational components as well as the extended Homeland Security Enterprise (HSE).

Within the ABT program, there are three focus areas:

- 1) ISR Sensors
- 2) Small UAS (Suas) Technology
- 3) C4 Operations (Command, Control, Communications, and Computers)

The focus area of ISR Sensors seeks solutions, processes, and means to advance the development and transition of ISR sensor technology applicable for HSE operational scenarios.

TOPIC RESEARCH SOUGHT: Type III

TRL SOUGHT: 1-7

TRL at CONCLUSION: 8

END OBJECTIVE:

The end objective of any ABT project is to transfer the advancement of aircraft technology (manned and/or unmanned) to enhance the mission capability of the DHS Operational Components and the extended HSE. The enhancement must be operationally relevant, measurable, beneficial, and consistent with the documented priorities and needs of the mission partner.

SEC BORD 03-06: Countering Unmanned Aircraft Systems

TOPIC DESCRIPTION:

The primary objective of this LRBA is to develop enhanced technologies and methods that allow for the detection, tracking, identification, and mitigation of unmanned aircraft systems

under varied terrains and environmental conditions such as, but not limited to:

- Dense urban environments
- Mass Gatherings (i.e. sporting events)
- Critical Infrastructure (i.e. bridges, power plants, reservoirs)
- Mobile platforms (i.e. moving vehicles, boats, aircraft)

New technologies and enhanced methods should be able to detect, track, identify and mitigate an array of unmanned aircraft threats and flight modalities that include, but are not limited to:

- Remote manual flight control using radio frequency-based transmissions
- Global navigation satellite system (GNSS) supported pre-programmed flights
- Autonomously pre-programmed flights that are unsupported by GNSS

TOPIC RESEARCH SOUGHT: Type II

TRL SOUGHT: 4 or higher

TRL at CONCLUSION: 7 or higher

END OBJECTIVE:

The end objective is to transfer the advancement of C-UAS technologies to enhance the mission capability of the DHS Operational Components and the extended Homeland Security Enterprise.

The enhancement must be operationally relevant, measurable, beneficial, and consistent with the documented priorities and needs of the mission partner.

Actionable Intelligence Gathering and Sharing (04)

SEC BORD 04-02: Non-Intrusive Screening to Detect Synthetic Opioids and Other Illicit Drugs

TOPIC DESCRIPTION:

Illicit drugs, such as fentanyl and other synthetic opioids, are entering the US at alarming rates. DHS requires the ability to non-intrusively screen bulk packaged materials (individual parcels/packages, mail bags, cargo, or containers) to detect synthetic opioids and other illicit drugs being smuggled into the United States at International Mail Facilities (IMFs), Express Consignment Centers (ECCs), and Border Ports of Entry (BPE). Topic seeks technologies that result in improvements to screening capabilities for end-users to include (1) advanced technologies that offer novel improvements or approaches to three-dimensional imaging; (2) algorithms or other analytical approaches to assist in operators in anomaly detection and reduce false alarms; and (3) technologies that will enable end-users to discriminate illicit materials from lawful materials to resolve alarms. Technologies are sought that enable end-users to conduct rapid, high-throughput inspection operations with minimal disruption to the flow of commerce and can be readily integrated into current Customs and Border Protection (CBP) field inspection operations.

TOPIC RESEARCH SOUGHT: Type III

TRL SOUGHT: 4-7

TRL at CONCLUSION: 6-8

END OBJECTIVE:

A technology that improves non-intrusive screening capabilities to detect and interdict illicit drugs with minimal disruption to the flow of commerce, is likely to be adopted by end users, and has a path to transition and/or commercialization.

Dark Aircraft and Vessel Detection, Tracking, and Interdiction (05)

SEC BORD 05-01: Sensors for Unmanned Maritime Systems

TOPIC DESCRIPTION:

DHS Science & Technology seeks innovative, capable, and reliable sensors to mount on small, commercially available unmanned maritime sensor platforms. The sensors are envisioned to be suitable for the size of the platform, require minimal power (less than 1,000 KVA), capable of functioning above and/or below the surface (as appropriate for the sensor type), and able to be integrated with the platform's communication system using non-proprietary data formats. Sensors are expected to surveil the surface and/or subsurface for a variety of threats (i.e. fast boats, chemical spills, subsurface vehicles, obstacles, etc.). Sensors are also required to classify the detected object. Sensor system need to be less than 3 kg and marinized for ocean environments.

TOPIC RESEARCH SOUGHT: Type III

TRL SOUGHT: 7-9

TRL at CONCLUSION: 8-9

END OBJECTIVE:

DHS S&T seeks TRL 7-9 technologies to provide sensor capability to existing unmanned maritime system platforms. In the end state, sensors and sensors platforms are envisioned to integrate with existing government command and control systems to aid in the detection, classification, and resolution of maritime threats.

Expedited People Screening (06)

Maritime Surveillance and Communications in Remote Environments (07)

SECURING CYBERSPACE (SEC CYB)

DHS has identified strengthening the security and resilience of cyberspace as a priority in its Quadrennial Homeland Security Review efforts. Priority areas for safeguarding and securing cyberspace are:

- Strengthen the security and resilience of critical infrastructure
- Secure the federal civilian government information technology enterprise
- Advance law enforcement, incident response and reporting capabilities
- Strengthen the ecosystem:
 - Drive innovative and cost-effective security products, services and solutions throughout the cyber ecosystem
 - Conduct and transition research and development, enabling trustworthy cyber infrastructure
 - Develop skilled cybersecurity professionals
 - Enhance public awareness and promote cybersecurity best practices
 - Advance international engagement to promote capacity building, international standards and cooperation

DHS S&T identifies, develops and delivers new cybersecurity technologies, tools, techniques, and next-generation capabilities that enable DHS and the nation to defend and secure current and future critical systems and networks against cyberattacks. We leverage public-private partnerships to identify real-world requirements for innovative technology solutions, which are developed with the partners and transitioned into the marketplace. Some examples of priority cybersecurity R&D needs include:

- Distributed cloud-based communications and monitoring
- Industrial control systems, cyber sensors, analytics, and prevention
- Metrics for cybersecurity effectiveness, severity, and comparison
- Data capture of networked devices for forensic examination Website: www.dhs.gov/cyber-research

Distributed Cloud-based Communications and Monitoring – Associated/Related Efforts (01)

Human Aspects of Cybersecurity-Associated/Related Efforts (02)

SEC CYB 02-03: Cyber Risk Economics (CYRIE)

TOPIC DESCRIPTION:

Cybersecurity is a multidimensional problem that demands interdisciplinary attention. The CYRIE program supports research into the business, legal, technical, and behavioral aspects of the economics of cyber threats, vulnerabilities, and controls. CYRIE R&D emphasizes empirically based measurement, modeling, and evaluation of:

- Investment into cybersecurity controls (technology, regulatory, and legal) by private-sector, government, and private actors
- Impact of investment on the probability, severity, and consequences of actual risks and resulting cost and harm
- Value of the correlation between business performance measures and evaluations of cybersecurity investments and impacts
- Incentives to optimize the investments, impacts and value basis of cyber risk management

TOPIC RESEARCH SOUGHT: Type III

TRL SOUGHT: 2-5

TRL at CONCLUSION: 6

END OBJECTIVE:

Priority R&D needs for this program are analytics and metrics for cybersecurity effectiveness, severity, and comparison. The CYRIE program endeavors to improve value-based decision making by those who own, operate, protect, and regulate the nation's vital data assets and critical infrastructure. As such, the program looks beyond the traditional economics view of incentives for cybersecurity, where individuals are assumed to be rational actors who know how to maximize their well-being, and considers a broader array of factors that include business, legal, technical, and behavioral factors. In this way, CYRIE R&D can more effectively address strategy and tactics for cyber risk avoidance, acceptance, mitigation, and transfer.

Network and Systems Security-Associated/Related Efforts (03)

SEC CYB 03-01: Distributed Denial of Service Defense (DDoSD)

TOPIC DESCRIPTION:

Distributed Denial of Service Defense and Telephony Denial of Service Defense (DDoSD/TDoSD) – Denial of service attacks are pervasive and have the potential to disrupt critical network infrastructure. Proposals that identify, provide situational awareness for, mitigate, provide recovery techniques, or protection for networks such as the Internet, enterprise networks, emergency communications [e.g. Next Generation 9-1-1 (NG911)], or other critical infrastructure networks are of interest. Situational Awareness, identification of, mitigation, recovery, and protection for communication channels such as voice, text, video, or other communication that may be received by NG911 are also of interest.

TOPIC RESEARCH SOUGHT: Type II

TRL SOUGHT: 4 or higher

TRL at CONCLUSION: 8-9

END OBJECTIVE:

The end goal is mitigation of Distributed Denial of Service (DDoS) attacks or protection for relevant networks and communication channels from Denial of Service attacks.

Efforts that provide tools and/or techniques for situational awareness and identify Denial of Service (DoS) attacks on relevant networks and communications channels, including differentiating between DDoS and other disruptions on relevant networks are of interest. These disruptions may occur at various layers of the network.

Efforts that provide mitigation techniques/tools, recovery techniques/tools, or protection to relevant networks and communication channels are also of interest. These efforts may leverage existing policies and practices or adopt existing technologies for near term protection. Novel

approaches for understanding and mitigating new forms of DDoS against relevant networks and communication channels are encouraged.

SEC CYB 03-02: Federated Enterprise Environments (formerly Cloud Computing Security)

TOPIC DESCRIPTION:

Research and Development to build upon security in Federated Enterprise Environments including secure protocols to protect data flow to, within and out of the federated environment; command and control (C2) infrastructure for federated environments; incorporation of adaptive defenses into federated environments; preserving data integrity; privacy constraints; privacy-preserving computation/contract generation; and systems to identify unauthorized activity.

TOPIC RESEARCH SOUGHT: Type III

TRL SOUGHT: 4-7

TRL at CONCLUSION: 8

END OBJECTIVE:

Research and development results of this topic should provide innovative technologies, techniques, and processes towards the creation, operation, and maintenance of federated enterprise environments and the related C2 infrastructure. Objectives include enabling local decision making given global knowledge and the seamless incorporation of various cybersecurity technologies and techniques (Moving Target/Dynamic/Adaptive Defenses, privacy preserving and multi-party computing, deception, etc.) into federated enterprise environments. Results are also sought to protect any cloud-based infrastructure that enables federated enterprise environments. Results are also sought to protect any cloud-based infrastructure that enables federated enterprise environments.

SEC CYB 03-04: Predictive Analytics

TOPIC DESCRIPTION:

Predictive Analysis, as applied to cybersecurity, is the ability to identify potential cyber threat vectors and determine the probable course of action for each threat.

TOPIC RESEARCH SOUGHT: Type II

TRL SOUGHT: 4 or higher

TRL at CONCLUSION: 8-9

END OBJECTIVE:

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

types of cyber threats may be considered.

SEC CYB 03-05: Information Marketplace for Policy and Analysis of Cyber- risk & Trust

TOPIC DESCRIPTION:

The Information Marketplace for Policy and Analysis of Cyber-risk & Trust (IMPACT) project supports the global cyber risk research community by coordinating and developing real world data and information sharing capability tools, models, and methodologies. To accelerate solutions around cyber risk issues and infrastructure security, the IMPACT project enables empirical data and information sharing between and among the global cybersecurity research and development (R&D) community in academia, industry, and government. Importantly, IMPACT also addresses the cybersecurity decision-analytic needs of Homeland Security Enterprise (HSE) customers in the face of high volume, high-velocity, high-variety and/or high-value data through its network of Decision Analytics-as-a-Service Providers (DASP). These resources are a service technology or tool capable of supporting the following types of analytics: descriptive (what happened), diagnostic (why it happened), predictive (what will happen) and prescriptive (what should happen).

TOPIC RESEARCH SOUGHT: Type III

TRL SOUGHT: 2-5

TRL at CONCLUSION: 6

END OBJECTIVE:

The Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) Office of Mission Capability Support (MCS) Physical and Cyber Security (PCS) Division seeks to coordinate, enhance, and develop advanced data and information sharing tools, datasets, technologies, models, methodologies, and infrastructure to strengthen the capabilities of national and international cyber risk R&D. These data sharing components are intended to be broadly available as national and international resources to bridge the gap between producers of cyber risk-relevant ground truth data, academic and industrial researchers, cybersecurity technology developers, and decision makers to inform their analysis of and policymaking on cyber risk and trust issues.

SEC CYB 03-06: National Research Infrastructure of Cyber Security Experimentation

TOPIC DESCRIPTION:

When new or updated tools and techniques are developed, the first step is to test them in a restricted environment. Testing always reveals subtleties in the environment that mandate changes to any new tool or technique. The DETER is such an environment and is required for testing, especially for Distributed Denial of Service tools and techniques as they are developed.

TOPIC RESEARCH SOUGHT: Type III

TRL SOUGHT: 8-9

TRL at CONCLUSION: 9

END OBJECTIVE:

The primary objective is to have a mature testbed that can be used to test and validate claims from various projects, in particular the DDoSD projects.

The results of this topic will catalyze and support the research and development of advanced experimental research tools, technologies, and methodologies as broadly available national resources. Indicators of the success of this program objective will be the realization of experimental research capabilities and approaches that reach beyond today's state of the art.

SEC CYB 03-07: IMPACT Data Catalogue

TOPIC DESCRIPTION:

The Information Marketplace for Policy and Analysis of Cyber-risk & Trust (IMPACT) is a data catalogue with access protections.

TOPIC RESEARCH SOUGHT: Type III

TRL SOUGHT: 8-9

TRL at CONCLUSION: 9

END OBJECTIVE:

The end objective is to have data available for research, development, testing and training. The data shall be managed for access and to meet all data provider requirements.

The Information Marketplace for Policy and Analysis of Cyber-risk & Trust (IMPACT) project supports the global cyber-risk research community by coordinating and developing real world data and information sharing capabilities, tools, models, and methodologies. To accelerate solutions around cyber-risk issues and infrastructure security, the IMPACT project enables empirical data and information sharing between and among the global cybersecurity research and development (R&D) community in academia, industry, and government. Importantly, IMPACT also addresses the cybersecurity decision-analytic needs of Homeland Security Enterprise (HSE) customers in the face of high volume, high velocity, high variety, and/or high value data through its network of Decision Analytics-as-a-Service Providers (DASP). These resources are a service technology or tool capable of supporting the following types of analytics: descriptive (what happened), diagnostic (why it happened), predictive (what will happen), and prescriptive (what should happen).

Mobile Security-Associated/Related Efforts (04)

SEC CYB 04-02: Mobile Security & Resiliency R&D

TOPIC DESCRIPTION:

The research and development of creating or enhancing technologies to enable the secure and/or resilient use of mobile ecosystem technologies in support of the DHS mission. Areas of interest include: 5G, mobile supply chain, security analysis, mobile infrastructure resilience, emergency communications, mobile vulnerability analysis, mobile communication security

protocol analysis, and security.

TOPIC RESEARCH SOUGHT: Type I

TRL SOUGHT: 3

TRL at CONCLUSION: 7

END OBJECTIVE:

The development of technologies that secure and add resilience to the mobile ecosystem that support DHS use cases.

Critical Infrastructure – Associated/Related Efforts (05)

(Including Industrial Control Systems, Cyber Sensors, Analytics, and Prevention)

Software Assurance– Associated/Related Efforts (06)

SEC CYB 06-01: Software Assurance

TOPIC DESCRIPTION:

The research and development of tools and techniques to reduce vulnerabilities in software and to improve how security is addressed in the process of developing and vetting software applications.

TOPIC RESEARCH SOUGHT: Type III

TRL SOUGHT: 6 or higher

TRL at CONCLUSION: 9

END OBJECTIVE:

Develop or provide software assurance tools, including making combinations of tools easier to use and to understand the results of such tools. This may be provided as a cloud service or as a stand-alone product. Both static and dynamic analysis tools or access to tools are desired. Code coverage metrics should be provided for any tools proposed or supported.

Additional desired activities include improving the software assurance ecosystem in novel or unique ways. This allows for a broad spectrum of activities, limited only by the creativity of the proposer.

Cyber Security Outreach – Associated/Related Efforts (07)

SEC CYB 07-01: Cyber Security Education

TOPIC DESCRIPTION:

Applied research in key education and training areas to ensure the nation has a highly skilled cybersecurity workforce is important to maintaining its systems and networks and combating future cyberattacks. Other areas of interest include:

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

TOPIC RESEARCH SOUGHT: Type II

TRL SOUGHT: 2-5

TRL at CONCLUSION: 6

END OBJECTIVE:

The objective is to develop, demonstrate, and transition substantive and adaptive cyber security education models that impact organizations and infrastructures/sectors for the better. These models should address key dimensions of the challenge, such as multiple age levels, cyber security across multiple operational domains, and different kinds of threats. An overarching objective of this work is to support development of "learning organization" capabilities across all kinds of organizations and infrastructures/sectors. The models and associated technologies need to support cybersecurity competitions, education and curriculum development, and workforce training and development needs.

Cybersecurity for Law Enforcement-Associated/Related Efforts (08)

(Including Data Capture of Networked Devices for Forensic Examination)

Cyber Enabled Networked Physical Systems Security (09)

PREVENTING TERRORISM (PREV)

A hallmark of homeland security, the prevention of terrorist attacks runs through the mission of every component within DHS. Terrorist tactics continue to evolve and the threat of terrorism has become increasingly difficult to detect.

Priority R&D needs and topics in preventing terrorism are:

Organic Explosive Compound and Homemade Explosives Detection (01)

Improvised Explosive Device-related Anomaly Detection (02)

Automated Machine Learning (03)

Prevention (04)

PREV 04-02: Vehicle Ramming Mitigation Technology

TOPIC DESCRIPTION:

Terrorists and other violent extremists have demonstrated an interest in leveraging simple and less sophisticated methods to inflict harm and disrupt infrastructure operations. As highlighted by incidents both domestically and abroad, vehicle ramming has become a common attack vector that is difficult to prevent given there are few to no identifiable indicators.

TOPIC RESEARCH SOUGHT: Type I

TRL SOUGHT: 2

TRL at CONCLUSION: 5

END OBJECTIVE:

This project aims to develop a capability that can be commercialized to enhance security against the vehicle ramming threat, with particular emphasis on special events.

PREV 04-03: Threat Prevention

TOPIC DESCRIPTION:

The ability to prevent public safety threats and malign actors through the application of social science methods can include:

1. Research and development to improve the detection, analysis, understanding, and mitigation of the threats posed by terrorism and targeted violence, human trafficking, child exploitation and online disinformation;
2. Knowledge, tools and technologies to determine when individuals, groups, and movements are likely to engage in violence or illegal activity; and
3. What ideological, organizational, and contextual factors may influence acts of violence, illegal activity, the spread of online disinformation, and target selection.
4. How to build community resilience to public safety threats.

TOPIC RESEARCH SOUGHT: Type I

TRL SOUGHT: 4-7

TRL at CONCLUSION: 8-9

END OBJECTIVE:

DHS S&T seeks to ensure rigorous, high quality data to understand the nature of threats in the United States; provide independent, objective assessment of activities to ensure that DHS can continually improve and understand the outcomes, impacts, and unintended consequences of investments in threat prevention; and, ensure the most up-to-date scientific information from around the world is readily available to DHS and DHS enterprise decision-makers for science-informed policy and practice.

Advanced Analytics (05)

PREV 05-01: Advanced Analytics for Next Generation Homeland Security Missions

TOPIC DESCRIPTION:

The Data Analytics Technology Center (DA-TC) invests in research, innovative solutions, and emerging technologies to enable advanced analytics for Next Generation Homeland Security Missions. Facilitating data driven solutions demands cross-cutting work on computation, data management, advanced analytics, technical architecture, and the underlying policy and for using enterprise data sets for cross mission applications.

Areas of interest to DA-TC that focus on technical architecture include distributed storage systems, block chain applications for privacy protecting information sharing and analytics, and secure multi-party computation. Effective data analytics requires reliable data, so that DA-TC is also focused on solutions to enable data wrangling and preparation as well as entity resolution.

DA-TC investigates the potential of advanced and emerging analytics capabilities to support the Homeland Security Mission, including advanced computational concepts, analytics and visualization, machine learning and deep learning, human centered systems, analytics for the Internet of Things (IOT), large-scale analytics on publicly available information including social media, real-time analytics for multi-party, multi-latency, metro-scale networks, human-centered systems, and quantum information science.

Nearly all DA-TC research and development undertakings also have important policy implications. A few of DA-TC's areas of interest highlight the cross-cutting nature of technical and policy considerations such as countering foreign influence, cyber security and cyber-physical security, election security, infrastructure protection, emergency management, and decision support and business processes, advanced privacy and security concepts, and adversarial machine learning.

TOPIC RESEARCH SOUGHT: Type I

TRL SOUGHT: 1

TRL at CONCLUSION: 7

END OBJECTIVE:

Develop data analytic and quantum capabilities that will increase the Department's ability to leverage mission data for decision-making.

PROTECTING FROM TERRORIST ATTACKS (PROT)

Protecting the American people from terrorist threats and attacks is the reason DHS was created and remains our highest priority. Terrorists seek sophisticated means of attack, including chemical, biological, radiological, nuclear, and explosive (CBRNE) weapons, and

cyber-attacks. Biological threat security, in particular, focuses around the prevention of release as well as detection of and protection against biological threats and hazards known to pose particularly high risk to the nation.

Priority R&D needs and topics are:

Personal Protective Equipment for all CBRNE Hazards (01)

Modeling and Predictive Analytics for Decision Making (02)

Disease and Biological Threat Detection, Identification, and Classification in Field Operational Environments (03)

Biological Attack Verification (04)

MANAGING INCIDENTS (MGMT)

Incident Management encompasses emergency response and critical infrastructure security and resilience, to include the preparedness, response, and recovery needs of more than 70,000 state, local, tribal, and federal agencies and 16 critical infrastructure sectors.

Priority R&D needs and topics in support of incident management needs are centered on the following priorities:

Situational Awareness (01)

MGMT 01-01: Alerts, Warnings, and Notifications Program Planning

TOPIC DESCRIPTION:

Research and development of Alerts, Warnings, and Notifications (AWN) tools, materials, and strategies for State, Local, Territorial, and Tribal (SLTT) alert originators that foster more effective AWN program planning and reduced alerting delays.

TOPIC RESEARCH SOUGHT: Type II

TRL SOUGHT: 3-4

TRL at CONCLUSION: 7

END OBJECTIVE:

Conduct research and pilots; and develop Alerts, Warnings, and Notifications (AWN) program planning guidance on how to build an effective AWN Program (e.g., Standard Messaging Templates, Hazard Matrices, Training Standards, Metrics, and Advocacy Materials for key decision makers) with planning artifacts for State, Local, Territorial, and Tribal (SLTT) alert originators.

Communications (02)

MGMT 02-01: Resilient Position, Navigation, and Timing (PNT)

TOPIC DESCRIPTION:

Accurate position, navigation, and timing (PNT) information is important for the functioning of many critical infrastructure sectors. Disruption of PNT services can hamper the operational capabilities of critical infrastructure operations that rely on precision timing or positioning. This topic seeks technologies that can improve resilience for PNT end-users to include:

- 1) disruption alerting and mitigation technologies
- 2) technologies that will enable end-users to continue normal operations through timing disruption events
- 3) technologies that provide novel timing capabilities

Offerors should consider the operational environment of timing end-users in critical infrastructure and factors that would facilitate successful transition/adoption. These factors include, but are not limited to, ease of integration into existing operational environments, price, and reliability. These considerations should be part of an Offeror's transition strategy.

TOPIC RESEARCH SOUGHT: Type III

TRL SOUGHT: 7-9

TRL at CONCLUSION: 8-9

END OBJECTIVE:

A technology that improves PNT resilience is likely to be adopted by critical infrastructure PNT end-users and has a path to transition and/or commercialization.

MGMT 02-05: Low-cost tactical communication devices for information sharing in remote environments (Border Security Technology Solution)

TOPIC DESCRIPTION:

Low-cost tactical communication devices that interface with modern smartphones to enable secure sharing of position location information (PLI) and text messages in remote environments for increased situational awareness.

TOPIC RESEARCH SOUGHT: Type III

TRL SOUGHT: 6-9

TRL at CONCLUSION: 7-9

END OBJECTIVE:

By providing a low-cost device that interfaces wirelessly with modern smartphones, low bandwidth data including position location information (PLI), text messages and other customer-provided payloads can be transmitted and received by DHS users in remote environments that do not have commercial infrastructure like cell towers. This effort will enable tactical air, land, and maritime information sharing to provide agent safety and increase agent situational awareness.

MGMT 02-07: Measuring Impact of Foreign Influence Operations and Resilience Efforts to Mitigate

TOPIC DESCRIPTION:

No methodology exists to measure the impact of foreign influence operations on Americans or the effectiveness of measures put in place to mitigate the risk of foreign influence. In order to design and implement effective resilience measures, a baseline understanding of how foreign influence operations impact citizens and a methodology to measure the effectiveness of programs is required.

Designing robust metrics requires analysis of foreign influence along several dimensions, including both the physical and cyber. Given that much human activity today has both physical and cyber footprints, detecting bad activity would be harder if one focuses on one of the other only. Infrastructure Protection (IP) theft for example, typically involves both.

TOPIC RESEARCH SOUGHT: Type I

TRL SOUGHT: 2

TRL AT CONCLUSION: 5

END OBJECTIVE:

These metrics would be used to identify the most effective methods for building national resilience to foreign influence operations. The information would be used to design and implement programs and communications to mitigate the risk of foreign influence operations. This is particularly important to DHS' emphasis on building National resilience through public awareness and education. Messaging, tactics, target audience, and outreach can all be guided by these metrics and methodology.

MGMT 02-08: GMD and Nuclear EMP Critical Infrastructure Risk

TOPIC DESCRIPTION:

Extreme electromagnetic incidents caused by an intentional electromagnetic pulse (EMP) attack or a naturally occurring geomagnetic disturbance (GMD, also referred to as "space weather") could damage significant portions of the Nation's critical infrastructure. Although EMP can be generated by several means, high-altitude electromagnetic pulse attacks (HEMP) using nuclear weapons are of most concern because they may permanently damage or disable large sections of the national electric grid and other critical infrastructure control system. Similarly, extreme geomagnetic disturbances associated with solar coronal mass ejections (when plasma from the sun, with an embedded magnetic field, arrives at Earth) may cause widespread and long-lasting damage to electric power systems, satellites, electronic navigation systems, and undersea cables. The systems at risk may be directly impacted or affected by damage to the communications and control upon which they are dependent.

TOPIC RESEARCH SOUGHT: Type I

TRL SOUGHT: 2

TRL AT CONCLUSION: 5

END OBJECTIVE:

Any or all of the following:

- Threat and Hazard Modeling—Severe geomagnetic disturbance (GMD) and nuclear electromagnetic pulse (EMP) are large-scale, high-impact, low-frequency (HILF) events where we have limited historical data and experience. The lack of experience creates a heavy reliance on models and simulations of these events to guide the protection of critical infrastructure (CI) and to estimate post-event responses for recovery and restoration.
- Mapping of National Critical Functions to Critical Infrastructure Networks—National Critical Functions (NCF) provide a high-level definition of functions that need to be sustained to avoid serious disruption to national security and safety and economic activity.
- Identification of Key Critical Infrastructure Assets and Vulnerability Assessments—The CI networks that support the NCFs are composed of many subsystems, devices and components.
- Prediction of Critical Infrastructure Network Performance Under Extreme Conditions—The CI networks that support the NCFs often exhibit complex behavior governed by physics, control systems, and human operator intervention.
- Design of Critical Infrastructure Network Vulnerability Mitigations to Ensure NCF Performance—Resources for hardening or sparing CI network subsystems, devices and components are often limited, and the effect of these mitigations on the CI network, especially as it pertains to NCF PEMP, are often not straightforward due to complex network behavior.

Command, Control, Communications (03)

MGMT 03-01: Enhanced Incident Management Services to Support Interoperable Rich-Data Information Integration and Exchange

TOPIC DESCRIPTION:

S&T seeks R&D for standards-based, enhanced incident management solutions with an emphasis on data interoperability and seamless integration of next-generation, data-rich environments including, but not limited to, mobile data, sensors, IoT, voice, video, asset utilization and availability, and GIS data sources.

Research concept materials should:

- Use of cloud-based solutions to provide greater scalability and adaptability for future technological capabilities
- Platform that supports data interoperability and integration from diverse sources. Compatibility, where possible, with legacy and state-of-the-art edge network devices.
- Adoption of data hierarchy concepts (i.e. “authoritative data” concept from CAD architectures) as an organizing principle

- Utilize standards-based technology interfaces, promoting standards-based solutions rather than proprietary ones
- Demonstrably reduce life-cycle costs (acquisition, operations & maintenance, and technology refresh)
- Result in force-multiplier functionality for users across all public safety disciplines and at all jurisdictional levels.

TOPIC RESEARCH SOUGHT: Type III

TRL SOUGHT: 7

TRL AT CONCLUSION: 8

END OBJECTIVE:

The successful demonstration of data interoperability and integration of cloud-based solutions to support multi-agency dispatching, information sharing, and incident management. Solutions will result in enhanced functions for call taking, dispatch, resource management, situational awareness, intelligent data analytics, sensor integration, alerting, and provide common operating intelligence to streamline and expedite decisions while reducing response time and improving responder awareness and safety.

MGMT 03-02: CAD-to-CAD Interoperability

TOPIC DESCRIPTION:

Critical data supporting incident response and resource management decisions is often not available to all organizations responding to an emergency because the various Computer-Aided-Dispatch (CAD) systems supporting each agency's mission and the systems they interact with on a daily base are unable to electronically exchange that information. Most CAD technology in use today by first responders was not developed to be interoperable with other systems and no communication or data exchange standards are currently in widespread use. As a result, situational awareness may suffer, operational inefficiencies may be introduced that negatively impact the optimum response to an incident, and improvised interoperability is achieved by developing custom interfaces that can be very costly to develop and maintain. Therefore, there is a need to:

- Understand the CAD interoperability landscape today including its challenges.
- Define interoperability, associated requirements, and their specifications to encourage interoperability between different solutions in use within one or more public safety agencies and with other incident information management stakeholders.
- Evaluate standards for use, aimed at the achievement of increased interoperability to support a full complement of inter-operable emergency incident data exchanges between a variety of public safety systems (CAD-to-CAD, CAD-to-records management system, CAD-to-mobile data, and others).
- Determine conformance specifications, validating testing methodologies, and encourage agency inclusion of the specifications during the acquisition process to foster broader adoption.
- Leverage existing national systems if feasible.

- Make recommendations to other public safety organizations and/or committees. on actions and steps that need to be taken in a comprehensive report.
- A phased approach that includes a proof of concept/operational prototypes.

TOPIC RESEARCH SOUGHT: Type I

TRL SOUGHT:

A phased approach to achieve the end objective shall be established. Phase-I with TRLs 1 to 3 can be achieved through the items outlined on the topic description. Upon completion of Phase-I, research recommendations to the Government, public safety organizations and/or committees on actions and key steps that need to be taken should be provided in a comprehensive report. Phase-II shall look to achieve TRLs 4 to 7 extrapolating the best of ongoing or completed pilots in the recent past and use Phase-I findings. In addition, implement operational pilots and proofs of concepts based on Phase-I findings and new technology opportunities. Phase-III should layout a standard baseline for TRL 8 to 9 that would be scalable, duplicable, cost effective and commercially available.

TRLs Chart

TRL	TRL Definition
1	Basic principles observed and reported.
2	Technology concept and/or application formulated.
3	Analytical and experimental critical function and/or characteristic proof-of-concept.
4	Component and/or breadboard validation in laboratory environment.
5	Component and/or breadboard validation in relevant environment.
6	System/subsystem model or prototype demonstration in a relevant environment.
7	System prototype demonstration in an operational environment.
8	Actual system completed and qualified through test and demonstration.
9	Actual system proven through successful mission operations.

TRL AT CONCLUSION:

At the conclusion of this project, we envision a standard's-based system that is scalable, duplicable, and ready to be commercialized.

END OBJECTIVE:

The end objective is to achieve a very resilient public safety CAD-to-CAD ecosystem that is very efficient, interoperable, and supports multi-discipline response to regional, multistate, or national events.

Risk Assessment and Planning (08)

MGMT 08-01: Community Resilience Through Technology

TOPIC DESCRIPTION:

Supporting R&D through social media, crowdsourcing models, planning tools and templates,

trainings, architectures, and technologies to enhance community preparation, resilience, response, and recovery in the face of all-hazards. Improvements in these capabilities can include:

- 1) Improved risk awareness, communications, and information-sharing between emergency responders and public officials
- 2) Increased pre-event planning, tactical operations, and recovery through education and training methods to support the implementation of information-sharing tools and tactics (examples including but not limited to: social media and crowdsourcing technologies) during emergency response operations
- 3) Applied theoretical and empirical research into the properties of resilient Smart Cities and communities

TOPIC RESEARCH SOUGHT: Type II

TRL SOUGHT: 3-4

TRL AT CONCLUSION: 7

END OBJECTIVE:

Planning tools and templates, trainings, architectures, and technologies to enhance community preparation, resilience, response, and recovery through new and novel application(s) of all-hazards mitigation strategies.

5 | Process Detail

Source Registration

Potential sources must register on the DHS S&T LRBA Submission Portal before submitting research concept material to the Industry Engagement process.

The submission portal uses a simple step by step procedure to register your entity and submit required research concept materials. Should you encounter any issues a help desk is available to assist you.

Help Desk

Email: dhsbaa@reisystems.com

Phone: 703-480-7676

Support Hours: M-F 9:00 AM – 5:00 PM ET

Sources should carefully review the current solicitations listed in this announcement and on the DHS S&T LRBA Submission Portal for the topic that most closely aligns with your research concept. Review the topic's details and prepare to submit research concept materials using the Topic Number and Name located on the portal. A "submission" tab located next to your topic of interest will walk you through the submission process.

INDUSTRY ENGAGEMENT

Potential sources must participate in industry engagement with Program Managers (PMs) in order to be invited to participate in the two-phased proposal process. Industry engagement begins with the submission of research concept materials as described below. Industry Engagement procedures are time and cost-efficient methods for industry to market their resources, the Government to make meaningful contacts in the industry, and to identify relevant technology and technically qualified sources that can perform a LRBA topic. Limitations to the Government's engagement with potential sources includes:

- The Government will not be obligated by any discussion with a potential Source;
- PMs cannot guide the potential Source;
- PMs cannot provide additional topic information or details beyond those publicly available;
- PMs cannot provide responses to specific questions posed by a potential Source that is not already publicly available. In most cases additional time and coordination with a Contracting Officer is required;
- PMs cannot attempt to replace the potential source's original ideas with his or her own; and
- PMs cannot share ideas or technical solutions that were provided to him or her by another potential source

Research Concept Material Submission Information

Potential sources must submit research concept material to the DHS S&T LRBA Submission Portal consisting of:

- 3-page abstract describing the technology or research, why it is unique, and an overview of the company, its capabilities, and relevant experience.
- Quad Chart depicting: (See instructions in Attachment 1)
 - Projected total cost
 - Impact and relevance to DHS
 - Project highlights
 - Technical and milestone bullets
- **Optional** short video: Potential Sources have the option of submitting a link to a non- professionally prepared video of not greater than 4 minutes demonstrating TRL-4 and above research prototypes. (See instructions in Attachment 2)

Note: Do not include proprietary information in any of your research concept materials.

Industry Engagement Assessment

The Industry Engagement period is 10 days in length. Research concept material submitted to the LRBA Submission Portal will be assigned by the LRBA program office to the topic's PM. The PM will complete an assessment of the submitted research concept material and determine if a brief scientific discussion with the source is necessary to gain a better understanding of the submission.

The PM's assessment generally considers the following:

- Relevance and Operational Requirements
- Technical Merit
- Unique and Innovative
- Strategic Outcomes
- Affordability and Transition
- Timeframe
- Entity's ability to understand the problem and perform the work

At the conclusion of the industry engagement period, unique research concept material that meets DHS needs, priorities, strategy, and funding may be invited by a Scientific Review Officer to participate in the two phase proposal process. Notification is normally emailed through the LRBA submission portal within two days following the scientific discussion.

PHASE I-VIRTUAL PITCH

Overview

The Phase I-Virtual Pitch is a 35 day calendar period consisting of 14 calendar days for the offeror to prepare and submit required Phase I materials (referenced further below) to the DHS S&T LRBA Submission Portal and 21 calendar days for the Government to conduct the virtual pitch and confidence assessment.

Supporting Written Materials:

- Files shall not exceed 10 MB
- Virtual pitch material may contain proprietary information and must be appropriately marked
- 12 PowerPoint Slides (title page does not count in the 12 slide total)
- Updated quad chart

DHS will set the virtual pitch date, time, conference line, and URL for sources invited to submit to the Phase I-Virtual Pitch. The virtual pitch will be conducted via Adobe Connect and a dedicated conference phone line. Offerors may opt, but are not required, to project a video image of the presenter(s).

Phase I-Virtual Pitch Process and Assessment

DHS S&T will utilize the following standardized format for the virtual pitch.

- Segment 1: 20 minute uninterrupted pitch from the offeror
- Segment 2: 10 minute Government-only to discuss potential questions
- Segment 3: 15 minutes of questions and answers

The Phase I-Virtual Pitch will be presented to a Peer Review Panel consisting of a Scientific Review Officer and at least one additional subject matter panelists. Following the pitch, the Peer Review Panel will complete their evaluation based on the two criterion listed below. The Peer Review Panel's assessment will be based upon the following criterion:

Criterion I: Technical Topic Suitability. Includes consideration of issues such as: relevance to technical topic; the degree of innovation and potential to offer a significant increase in capability; and the ability to offer a significant reduction in cost over current technologies or processes.

Criterion II: Topic Strategic Outcome. Includes consideration of issues such as: meets S&T and/or Component objectives; benefits strategic outcomes; and the ability to demonstrate outcome in an operational environment.

Approximately two days following the virtual pitch, offerors will receive a notification letter.

PHASE II-WRITTEN PROPOSAL

The Phase II-Written Proposal is a 66 calendar day process consisting of a 45 calendar day period for the offeror to prepare and submit their written proposal to the DHS S&T LRBA Submission Portal; and a 21 calendar day period for the Government's Peer Review Panel to conduct a confidence assessment and subsequent award recommendation. The Phase II-Written Proposal shall include a Technical Volume and a Cost Volume.

Written proposals will only be accepted from offerors that have been invited by a Scientific Review Officer following the completion and assessment of the Phase I-Virtual Pitch.

Written Proposal-Submission Information

Invited offerors are advised of the following written proposal submission information and format:

- Proposal's technical volume may not exceed 25 single-sided pages;
- Proposal's cost volume does not have a page limitation
- Paper Size-8.5 x 11 inch paper;
- Margins-1 inch;
- Spacing-single or double spaced;
- Font-Times New Roman, 12 point;
- Convert the original document into a PDF file; and
- Files may not exceed 10 MB.

Technical Volume Format

- Cover Page (Not included in the page count – includes the following)

- BAA number 18-01;
 - Title of proposal;
 - Topic Research Area and its Topic Number;
 - Identity of the prime Offeror, including name and address, and complete list of subcontractors, including name and address, if applicable;
 - Technical contact (name, address, phone, electronic mail address);
 - Administrative/business contact (name, address, phone, electronic mail address);
 - Duration of effort (separately identify the basic effort and any options);
 - DHS S&T point of contact, if applicable;
 - Dunn & Bradstreet (DUNS) number;
 - Acknowledgement that the Offeror is registered in Central Contractor registration (CCR). This can be established at the System for Award Management (SAM) website at <https://www.sam.gov/portal/public/SAM/>;
 - Statement specifying compliance with FAR Clause 52.222-54 “Employment Eligibility Verification.”
- Confirmation of U.S. Citizenship for those participating in the project, and the identity of any proposed personnel or subcontractors who are not U.S. citizens.
 - Official Transmittal Letter with authorizing official signature. For an electronic submission, the letter can be scanned and incorporated into the electronic proposal. The letter of transmittal shall state whether this proposal has been submitted to another government agency other than DHS S&T and, if so, which one and when.
 - Table of Contents (Not included in the page count)
 - 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. 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 detailed explanation of how the proposed product(s) supports the targeted end user, its operational use and how it will improve operational performance or outcomes. Describe the proposed technical solution and operational concept for accomplishing the stated 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.

- **Technical Concept.** Provide 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. 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. What particular scientific, technical or engineering issues need to be addressed and resolved to demonstrate feasibility?
- **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 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.
- **Commercialization Plan:** If relevant, offerors must also include a description in

the proposal of their plan for commercializing the technology, or other plans for getting the technology into established transition paths. Technology transition plans that include commercial partnerships are preferred, but transition into the open source community is also acceptable. This request does not entail providing a full business plan, nor does it imply that DHS views commercialization activities as in the scope of the LRBAAs topic. The intent is for offerors to provide evidence that, as part of the technical plan development, consideration has been given to the ultimate commercialization of the outputs of DHS- funded programs. Such considerations would include expected user base, how the technology will be used, and how it will be transitioned, manufactured and distributed to broad use. Of key importance are the identification of technology diffusion paths that are appropriate for the type and maturity of the technology involved, and any additional factors that might increase the likelihood of it being commercialized. Offerors who intend to partner with other companies for manufacturing and distribution services should identify their partners and the partners' capabilities.

- 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.
- Employment Eligibility Verification. Include a statement specifying compliance with FAR Clause 52.222-54.
- Intellectual Property: (Not included in the page count) In accordance with the various intellectual property provisions contained in applicable award authorities, including FAR provisions for "Data Rights" and "Patent Rights" where a FAR-based contract will be awarded, include a summary of any assertions to any intellectual property rights, including technical data or computer software that will be developed or delivered under the resultant award. This includes assertions to pre-existing rights, prototypes, or systems supporting and/or necessary for use of the research, results, or prototype. Any rights asserted in other parts of the proposal (oral or written) that would impact the rights to the government must be cross referenced here. If any 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, 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.

Offerors responding to this LRBA must submit a separate list of all technical data or computer software according to the assertions table below as an attachment to its written proposal that will be furnished to the Government with other than unlimited rights. The Government will assume unlimited rights if offerors fail to identify any intellectual property restrictions in their proposals. Include in this section all proprietary claims to results, prototypes, and/or deliverables. If no restrictions are intended, then the offeror should state "NONE."

Assertions Table

For each deliverable listed in the below table, please identify any assertion of restriction on the Government's Use, release or disclosure of technical data or computer software.

Deliverable	Technical Data or Computer Software to be Furnished With Restrictions*	Basis for Assertion**	Asserted Rights Category***	Name of Person Asserting 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. For computer software or computer software documentation identify the software or documentation.

** Generally, development at private expense, either exclusively or partially, is the only basis for asserting restrictions. For technical data, other than computer software documentation, development refers to development of the item, component, or process to which the data pertain. The Government's rights in computer software documentation generally may not be restricted. For computer software, development refers to the software. Indicate whether development was accomplished exclusively or partially at private expense. If development was not accomplished at private expense, or for computer software documentation, enter the specific basis for asserting restrictions.

*** Enter asserted rights category (e.g., government purpose license rights from a prior contract, limited, restricted, or government purpose rights under this or a prior contract, or specially negotiated licenses).

**** Corporation, individual, or other person, as appropriate, or enter "none" when all data or software will be submitted without restrictions.

Completed by:

Signature
Printed Name

Date

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:”

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.

Detailed description of the asserted restrictions. For each of the technical data or computer software identified above, identify the following information:

- Asserted rights. Identify the asserted rights for the technical data or computer software.
- 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.
- 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.
 - Entity asserting restrictions. Identify the corporation, partnership, individual, or other person, as appropriate, asserting the restrictions.
- 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.

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

The Bayh-Dole Act shall apply for any patentable materials, technologies, or knowledge developed on a FAR-based contract resulting from this LRBA and may apply in the case of an Other Transactions Agreement. The Government reserves nonexclusive, perpetual, royalty-free licensure of any materials developed under any contract or agreement resulting from this LRBA.

The government reserves the right to require delivery of additional data within the scope of the project that is not otherwise specified in the agreements as authorized to be withheld within a period of three years after acceptance of all items to be delivered. Any conversion to into a prescribed form, reproduction or delivery will be compensated.

Ineligibility for award. An Offeror's failure to submit or complete the identifications and assertions required by this provision with its offer may render the offer ineligible for award.

This section must be severable, i.e., it will begin on a new page and the following section shall begin on a new page. It is anticipated that the proposed Assertion of Data Rights will be incorporated as an attachment to the resultant award instrument. To this end, proposals must include a severable self-standing Assertion of Data Rights without any proprietary restrictions, which can be attached to the contract or agreement award. This Assertion of Data Rights will not count against page limit for written proposals.

Price/Cost Volume Format

- Cover Page: The cover page is automatically generated during the submission of the Industry Engagement materials to the DHS S&T LRBAAs Submission Portal. This is NOT the same as the Offeror's cover page.
- The price/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):
 - 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).
 - 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.)
 - Identify any cost drivers.
 - Options must be separately priced.

Cover Page: The use of the SF 1411 is optional. The words “Price/Cost Proposal” must appear on the cover page in addition to the following information:

- LRBAAs Number 18-01;
- Title of proposal;
- Topical area and reference code;
- Identity of prime Offeror, including name and address, and complete list of subcontractors, including names and addresses, if applicable;
- Technical contact (name, address, phone/fax, electronic mail address);
- Administrative/business contact (name, address, phone/fax, electronic mail address);
- Duration of effort (separately price out the basic effort and any options);
- DUNS number and CAGE code;
- 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;
- DCAA point of contact (name, telephone number, and email address);

Cost Proposal Part 1

- Part 1 of the cost proposal must include a detailed breakdown of all costs by cost category by calendar and Government fiscal year and include a summary explaining how each element is applied in the cost proposal:
- Direct Labor: Individual labor category or person, with associated labor hours

and unburdened direct labor rates.

- Indirect Costs: Fringe Benefits, Overhead, G&A, COM, etc. (Must show base amount and rate).
- (If applicable and available) Forward Pricing Rate Agreement (FPRA) or Defense Contract Audit Agency (DCAA) approved or recommended rates. Identify if there are outstanding CAS violations. Offerors please note the following:
 - In order to qualify for the award of a cost reimbursement contract, the offeror must have an adequate accounting system in accordance with FAR 16.301- 3(a)(1). Evidence of an adequate accounting system would include a written opinion or other statement from the cognizant federal auditor (CFA) or the cognizant federal agency official (CFAO) that the system is approved or has been determined to be adequate. If available, the offeror shall provide the audit report number and date associated with the accounting system review. If the offeror does not have a copy of the report, the offeror may furnish a copy of the audit report number.
 - If the offeror does not have an accounting system that has been determined adequate by the CFA or CFAO, but believes its accounting system is adequate, the offeror shall so state in its proposal. As part of the pre-award evaluation process, the Government will obtain the necessary review by the CFA. The offeror will be required to allow the CFA to review the accounting system and correct (or have a timely action plan to correct) any issues identified as precluding the system from being adequate. The offeror will provide the CFA name, address and telephone number and the point of contact as part of its proposal.
 - Offers will be rejected if the offeror does not have an adequate accounting system unless the Government determines that the offeror's action plan for correcting the accounting system is timely and acceptable. However, no costs will be paid under the contract until the Contractor's system has been determined adequate.

Adequacy of the Accounting System

In order to qualify for the award of a FAR-based contract with a contract type other than firm-fixed-price, the offeror must have an adequate accounting system in accordance with FAR 16.104(i).

- Evidence of an adequate accounting system would include a written opinion or other statement from the cognizant federal auditor (CFA) or the cognizant federal agency official (CFAO) that the system is approved or has been determined to be adequate. If available, the offeror shall provide the audit report number and date associated with the accounting system review. If the offeror does not have a copy of the report, the

offeror may furnish a copy of the audit report number.

- If the offeror does not have an accounting system that has been determined adequate by the CFA or CFAO, but believes its accounting system is adequate, the offeror shall so state in its proposal. As part of the pre-award evaluation process, the Government will obtain the necessary review by the CFA. The offeror will be required to allow the CFA to review the accounting system and correct (or have a timely action plan to correct) any issues identified as precluding the system from being adequate. The offeror will provide the CFA name, address and telephone number and the point of contact as part of its proposal.
- Offers will be rejected if the offeror does not have an adequate accounting system unless the Government determines that the offeror's action plan for correcting the accounting system is timely and acceptable. However, no invoices will be paid under the contract until the Contractor's system has been determined adequate.
- The Contractor shall maintain an adequate accounting system to substantiate vouchers (including any subcontractor hours reimbursed at the hourly rate in the schedule) by evidence of actual payment and by:
 - Individual daily job timekeeping records;
 - Records that verify the employees meet the qualifications for the labor categories specified in the contract; and
 - Other substantiation approved by the Contracting Officer.

Special Instructions for Time and Materials (T&M) and/or Labor Hour (LH) Proposals

- **Hourly Rate.** List the labor categories that will be used in performance of the work, the qualifications for each labor category, and the hourly rate that shall be paid. Use the guidelines at FAR 52.232-7, Payments under Time-and-Materials and Labor-Hour Contracts. The hourly rates shall include wages, indirect costs, general and administrative expense, and profit.
- **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. Identify materials as direct materials, subcontracts for supplies or incidental services, other direct costs (including travel), and indirect costs.
- **Direct Materials.** Describe the materials that will enter directly into the end product, or that will be used or consumed directly in connection with the furnishing of the end product or service.

- **Other Directs Costs.** List and describe 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.
- **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.
- **Subcontractor Cost Proposals.** 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.
- **Indirect Costs.** Describe indirect costs that will be charged to direct materials, subcontracts for supplies or incidental services, or other direct costs. Describe the basis for calculating each indirect cost.
- Spend Plan must 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 providing 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 II

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

The Price/Cost Proposal should be consistent with your proposed SOW. Activities such as demonstrations required to reduce the various technical risks should be identified in the SOW and reflected in the Price/Cost Proposal. The Offeror should provide a total estimated

price for the major Research, Development, Test, and Evaluation (RDT&E) activities associated with the program.

Phase II-Written Proposal-Confidence Assessment and Notification

A Peer Review Panel comprised of a Scientific Review Officer and one or more additional subject matter panelists will conduct confidence assessments. The Scientific Review Officer will then conduct a consensus discussion and complete a consensus evaluation. The timeframe for reviewing the written proposal and completing the Peer Review is 21 days.

The Phase II-Written Proposal is based on the following criterion:

Criterion I: Technical Approach. Confidence rating based on the overall scientific and technical merit including the quality, depth and thoroughness of the proposed technical approach and techniques and to what extent the proposal clearly provides sufficient detail for the Government to understand and evaluate the nature of the technical approach.

Criterion II: Management Approach. Confidence rating based on the proposed project management, understanding of risk, mitigation of risk, the proposed process to demonstrate the technical outcome in an operational environment and to what extent the proposal clearly demonstrates how the offeror intends to manage and accomplish the project and provides sufficient detail for the Government to understand and evaluate the nature of the management approach.

At the conclusion of the Phase II-Written Proposal, offerors will be provided a notification letter. Electronic notification is made through the LRBA portal within five (5) calendar days following the Peer Review Panel's consensus evaluation. Offerors not recommended for an award will be provided written technical feedback by the Scientific Review Officer.

Award Requirements

A Peer Review Panel's award recommendation is subject to agreement between the parties on the terms and conditions of the award.

The following represents those requirements that must be recognized and fully met prior to an award being made.

- NAICS: The North American Industry Classification System (NAICS) code for this announcement is 541715 (Research and Development in the Physical, Engineering, and Life Sciences (except Nanotechnology and Biotechnology) with a small business size standard of 500 employees.
- SAM.gov: Successful Offerors not already registered in the System for Award Management (SAM.gov) will be required to register prior to award of any grant, contract, cooperative agreement, or other transaction agreement. Information regarding registration is available at the following address <https://www.sam.gov/portal/public/SAM/>.
- Certifications: In accordance to FAR Part 4.11, all prospective contractors shall

be registered in the System for Award Management (SAM) prior to award. The SAM is the official U.S. government system that consolidates the capabilities of CCR/FedReg, ORCA and EPLS. There is NO fee to register for SAM. If you used any of the previous systems, you should now go to www.sam.gov to update your information. SAM training tools and quick-start guides are available on both the SAM and Federal Service Desk websites, located at www.sam.gov and www.fsd.gov.

Federal Travel Regulations (FTR): Information on per diem rates based on travel locations are provided on www.gsa.gov. Also, refer to FAR PART 31 for information on travel costs.

6	Other Information
----------	--------------------------

Test and Evaluation Facilities

Department of Homeland Security Science & Technology Directorate may make available appropriate test and evaluation facilities to support this program. Offerors should provide any specific requirements needed for test and evaluation of their proposed concept in their white papers and proposals.

Certificate of Current Cost or Pricing Data

Successful contract proposals that exceed \$750,000.00 may require the submission of a Certificate of Current Cost or Pricing Data in accordance with FAR 15.403-4(b)(2), prior to award.

Government Property, Government Furnished Equipment (GFE) and Facilities

The Government may provide government-furnished equipment (GFE), resources (GFR), information (GFI), or services (GFS) under the terms of each negotiated contract or agreement. GFE, GFR, GFI, or GFS requested by an Offeror must be factored into the Offeror's project cost. Each Offeror must provide a very specific description of any equipment or hardware it needs to acquire to perform the work. This description should indicate whether or not each particular piece of equipment or hardware will be included as part of a deliverable item under the resulting award. In addition, this description should identify the component, nomenclature, and configuration of the equipment or hardware that it proposes to purchase for this effort. The Government wants to have the contractor purchase the equipment or hardware for deliverable items under its contract. It will evaluate case-by-case the purchase, on a direct reimbursement basis, of special test equipment or other equipment, not included in a deliverable item, will be evaluated for allowability on a case-by-case basis. Maximum use of Government integration, test, and experiment facilities is encouraged in each of the Offeror's proposals.

Government research facilities may be available and should be considered as potential GFE. These facilities and resources are of high value, and some are in constant demand by multiple

programs. The use of these facilities and resources will be negotiated as the program unfolds. Offerors should explain which of these facilities they recommend and why. If any prototype, instrument or device that is produced during the period of performance of a funded project, one or more samples shall be delivered to DHS S&T CBD before the end of the period of performance for demonstration purposes. More specific information about the provision of a sample(s) will be incorporated in the Statement of Work.

SAFETY Act

As part of the Homeland Security Act of 2002, Congress enacted the Support Anti- Terrorism by Fostering Effective Technologies Act of 2002 (the “SAFETY Act”). The SAFETY Act puts limitations on the potential liability of firms that develop and provide qualified anti-terrorism technologies. DHS S&T, acting through its Office of SAFETY Act Implementation (OSAI), encourages 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 OBAA are encouraged to submit SAFETY Act applications for their existing technologies. They are invited to contact OSAI for more information, at 1-866-788-9318 or helpdesk@safetyact.gov. They also can visit OSAI’s Web site at www.safetyact.gov.

Export Control Considerations

International Traffic in Arms Regulations (ITAR) may apply to one or more of the TTAs in this OBAA. Foreign nationals must meet the requirements for participation set by those regulations, if required.

Hazardous Materials

Depending on the topic and in accordance with applicable FAR and DHS hazardous material clauses to be incorporated under any resultant contract award, offeror may choose to or be required to utilize hazardous materials during the course of the project development effort. If the government provides hazardous samples as part of the developmental and operational testing, information on the samples will be provided to the successful offerors requiring such samples.

Hazardous material, as used here, includes any material defined as hazardous under the latest version of Federal Standard No. 313 (including revisions adopted during the term of the contract). If the successful offerors choose to use their own hazardous samples, offerors must meet the requirements for the identification and material safety as follows:

HAZARDOUS MATERIAL IDENTIFICATION AND MATERIAL SECURITY DATA

- (a) “Hazardous material,” as used in this section, includes any material defined as hazardous under the latest version of Federal Standard No. 313 (including revisions adopted during the term of the contract).
- (b) The Offeror must list any hazardous material, as defined in paragraph (a) of this

clause, to be delivered under this contract. The hazardous material shall be properly identified and include any applicable identification number, such as National Stock Number or Special Item Number. This information shall also be included on the Material Safety Data Sheet submitted under this contract. This list must be updated during performance of the contract whenever the Contractor determines that any other material to be delivered under this contract is hazardous.

Material (If none, insert "None") Identification No.

_____	_____
_____	_____
_____	_____

- (c) The apparently successful Offeror agrees to submit, for each item as required prior to award, a Material Safety Data Sheet, meeting the requirements of 29 CFR 1910.1200(g) and the latest version of Federal Standard No. 313, for all hazardous material identified in paragraph (b) of this clause. Data shall be submitted in accordance with Federal Standard No. 313, whether or not the apparently successful Offeror is the actual manufacturer of these items.
- (d) Failure to submit the Material Safety Data Sheet prior to award may result in the apparently successful Offeror being considered non-responsible and ineligible for award.
- (e) If, after award, there is a change in the composition of the item(s) or a revision to Federal Standard No. 313, which renders incomplete or inaccurate the data submitted under paragraph (d) of this clause, the Contractor shall promptly notify the Contracting Officer and resubmit the data.
- (f) Neither the requirements of this clause nor any act or failure to act by the Government shall relieve the Contractor of any responsibility or liability for the safety of Government, Contractor, or subcontractor personnel or property.
- (g) Nothing contained in this clause shall relieve the Contractor from complying with applicable Federal, State, and local laws, codes, ordinances, and regulations (including the obtaining of licenses and permits) in connection with hazardous material.
- (h) The Government's rights in data furnished under this contract with respect to hazardous material are as follows:
 - (1) To use, duplicate and disclose any data to which this clause is applicable. The purposes of this right are to –
 - i. Apprise personnel of the hazards to which they may be exposed in using, handling, packaging, transporting, or disposing of hazardous materials;
 - ii. Obtain medical treatment for those affected by the material; and
 - iii. Have others use, duplicate, and disclose the data for the Government for these purposes.
 - (2) To use, duplicate, and disclose data furnished under this clause, in accordance with paragraph (h) (1) of this clause, in precedence over any other clause of this contract providing for rights in data.

- (3) The Government is not precluded from using similar or identical data acquired from other sources.
- i. Except as provided in paragraph (i)(2), the Contractor shall prepare and submit a sufficient number of Material Safety Data Sheets (MSDS's), meeting the requirements of 29 CFR 1910.1200(g) and the latest version of Federal Standard No. 313, for all hazardous materials identified in paragraph (b) of this clause.
- (4) For items shipped to consignees, the Contractor shall include a copy of the MSDS's with the packing list or other suitable shipping document which accompanies each shipment. Alternatively, the Contractor is permitted to transmit MSDS's to consignees in advance of receipt of shipments by consignees, if authorized in writing by the Contracting Officer.
- (5) For items shipped to consignees identified by mailing address as agency depots, distribution centers or customer supply centers, the Contractor shall provide one copy of the MSDS's in or on each shipping container. If affixed to the outside of each container, the MSDS's must be placed in a weather resistant envelope.

7

Contacts

LRBAA Role	Name	Phone	E-mail
Contracting Officer	Jenista M. Tobias	202-447-0721	Jenista.Tobias@hq.dhs.gov
Program Office	Dusty Lang	202-254-6837	lrbaa.admin@hq.dhs.gov

DHS S&T LRBAA Website:

<https://baa2.st.dhs.gov>

DHS S&T LRBAA Website Help Desk:

dhsbaa@reisystems.com

703-480-7676

Support Hours: Monday-Friday

9:00 AM – 5:00 PM ET

8

LRBAA Announcement 18-01 Attachments

Attachment No.	Attachment Title
1	Quad Chart Instructions
2	Virtual Pitch Instructions
3	
4	
5	
6	
7	

Attachment 1 (Quad Chart Instructions)

Quad Chart Instructions

The Quad Chart is used to provide a synopsis of the proposed project objectives and progress, as well as providing a graphical representation of the project. The Quad Chart is one landscape-oriented page divided into four quadrants. Emphasis will be placed on brevity and factual statements. Also, technical engineering details are not included.

- Sources may NOT include proprietary information on the quad chart submitted during the Industry Engagement process.
- Sources will have the opportunity to update their quad chart and include proprietary information if they are invited to submit to the Phase I Virtual Pitch proposal process.

Each of the four quadrants that comprise the Quad Chart conveys information on a specific aspect of the project. The first quadrant, located in the upper left-hand corner, comprises visually appealing graphics or pictures that clearly represent the key technological idea(s) or the expected impact of the research. If more than one picture is needed to clearly convey the technological idea(s), then a plurality of pictures may be used. Due to the limited space, the number of graphics and pictures should be limited to a maximum of five. If a plurality of pictures is included, they can be presented in any clear, appealing layout, such as a simple array of pictures or a collage of overlapping of pictures. However, they must fit neatly within the first quadrant. There may be something subtle or non-obvious to the casual observer in one or more of the pictures. If this is the case, graphics, such as red arrows, may be added to bring attention to important aspects of the picture(s).

The second quadrant (Project Description), located in the upper right-hand corner, includes a brief project description. A bulleted list format is used to present this information. For purposes of brevity, the description should be limited to a maximum of five bullets.

The third quadrant (Impact), located in the lower left-hand corner, includes three to five quantitative statements discussing how the project work will revolutionize an area of importance to DHS.

The fourth quadrant (Technical, Schedule & Cost), located in the lower right-hand corner, includes three technical and three milestones along with the projected cost of the research project.

The Quad Chart also includes a project title that is clearly visible and centered at the top of the page. The Quad Chart concludes with the LRBA Topic Number and Name in the bottom left-hand corner and the Offeror's name and Entity in the bottom right-hand corner.

Quad Charts will only be accepted in Microsoft PowerPoint formats converted to PDF. The Quad Charts are limited to one page, and the file size is limited to 500,000 bytes (0.5 MB). Quad charts are meant to be a capabilities and technology overview and should not include

any proprietary information.

The quad chart should briefly convey the following information as relevant to your idea:

- What are you trying to accomplish?
- How is it done now, with what limitations?
- What is truly new in your approach which will remove current limitations and improve performance? How much will performance improve?
- If successful, what difference will it make?
- What are the mid-term, final exams or full-scale applications required to prove your hypothesis? When will they be done?
- How could this transition to the end user?
- How much will it cost?

XYZ System

<p>PICTURE(S) OR GRAPHIC(S)</p>	<p><u>Project Description</u></p> <ul style="list-style-type: none">• XXXXXX• XXXXXX• XXXXXX• XXXXXX• XXXXXX
<p><u>Impact</u></p> <ul style="list-style-type: none">• XXXXXX• XXXXXX• XXXXXX• XXXXXX• XXXXXX	<p><u>Technical</u></p> <ul style="list-style-type: none">• XXXXXX• XXXXXX• XXXXXX <p><u>Milestones</u></p> <ul style="list-style-type: none">• XXXXXX• XXXXXX• XXXXXX <p><u>Projected Cost</u></p> <ul style="list-style-type: none">• XXXXXX
<p>LRBAA Topic Number & Name</p>	<p>Offerors Name, Entity</p>

Video Pitch Instructions

NOTE: Submission of an accompanying video pitch with Industry Engagement research concept materials is optional.

- 1.0 Potential sources submitting to the industry engagement process have the option of submitting a link to a short (up to 4 minute) video to support Technology Readiness Level (TRL) 4 and above capability statements described in the required 3 page written abstract. TRL definitions may be found at the following link:
<https://www.dhs.gov/sites/default/files/publications/product-realization-guide-partnership-focus-508-1.pdf>
Potential sources:

- 1.1. **May not include proprietary information or sensitive information, or otherwise make the video with any restrictive language regarding use;**
- 1.2. Are highly discouraged from preparing and submitting a studio or professionally prepared video. The preferred method for recording a video is with a smartphone or video camera; and
- 1.3. May film an effective video using only their smartphone. Special lighting and sound equipment is not required. The web provides many tutorials, recommendations and processes for recording and editing.

2.0 Considerations

- 2.1. Keep the video concise and simple. The video is intended to support TRL 4 and above statements made in your research concept material.
- 2.2. Keep your impact and benefit statements to one to two sentences. Address this in more detail within the research concept material's abstract.
- 2.3. Familiarize yourself with tips and processes for creating effective short videos.
- 2.4. Devote a majority of your time to demonstrating how the prototype or idea is addressing the topic's problem.
- 2.5. Don't discuss your company or researchers. That is what the industry engagement's abstract is intended to address.
- 2.6. Your prototype does not have to work flawlessly or look great. Concentrate on getting your message across.

3.0 Instructions for uploading the video to YouTube

- 3.1. Record the video;
- 3.2. Go to YouTube.com and register/sign-in;
- 3.3. Click “upload” in the upper-right corner;
- 3.4. Click the large arrow above “select files to upload”;
- 3.5. Choose your file; (Compatible files include: MOV, MPEG4, MP4, WMV)
- 3.6. All videos will be submitted via an “unlisted” YouTube link; and
- 3.7. Upload the video and include the unique URL in your research concept abstract.
 - 3.7.1. YouTube is inherently a public website and by that nature your submitted video is considered public.
 - 3.7.2. Do not include proprietary information in your video and do not mark or otherwise utilize restrictive language with regard to public use. Submissions that convey such restrictions will not be accepted, and DHS is not responsible for enforcement of any restrictions.
 - 3.7.3. Do not state in the video description, title, or tags that the video is unlisted.
- 3.8. Additional information may be obtained by visiting YouTube’s Help Page at: https://support.google.com/youtube/answer/57407?hl=en&ref_topic=2888648