APPENDIX A – RESEARCH TOPIC DESCRIPTIONS

SBIR Topic Number: DHS201-001

TITLE: Next Generation 9-1-1 (NG9-1-1) Multimedia content analysis engine capability for the Emergency Communications Cyber Security Center (EC3)

TECHNOLOGY AREAS: *Cybersecurity, Artificial Intelligence (AI), Analytics, Next Generation 9-1-1 (NG9-1-1), Voiceover Internet Phone (VoIP), Session Initiation Protocol*

OBJECTIVE: To establish approaches, develop, demonstrate, or pilot technology for implementing the security, and content analysis of multimedia messages from the public to the NG9-1-1 Public Safety Answering Point (PSAP) EC3 within NG9-1-1 Emergency Service Internet Protocol Networks (ESINets).

DESCRIPTION: As public safety answering points (PSAPs) adopt Next Generation 9-1-1 technology and are interconnected via regional Internet Protocol networks, it is important to establish standards and best practices to minimize the risk of cyber-attacks and to ensure appropriate and robust NG9-1-1 system security, as well as maintaining complete interoperable features and promoting better situational awareness and operational/incident coordination. Currently PSAPS have minimal capabilities for analyzing multi-media 9-1-1 data, and the timing of this project would coincide with the initial first PSAPS having the capability to receive multimedia content which must be properly analyzed prior to the PSAP opening and possibly jeopardizing the integrity of the 911 center.

The Federal Communications Commission (FCC) Task Force on the Optimal PSAP Architecture recommends a National Network Security Operations Center be established to coordinate cybersecurity across the NG9-1-1 landscape in the US. This national level entity could assist with defining NG9-1-1-specific policy related to cybersecurity for public safety networks and would benefit greatly from the enhanced situational awareness and security the technology developed under this SBIR project could provide. Additional lower level SOC's could deploy this technology for use in their PSAP, regional, state or nationwide NG911 networks. One of the new and evolving threats NG9-1-1 will bring is the possibility of malicious content in multimedia messages originating from the public. There is the need for technologies that can assist in the content and security analysis of these messages originating from the public in a time critical manner.

The EC3 concept includes small to medium units supporting multiple small or medium size PSAPS, as well as larger units capable of supporting multiple medium to large PSAPS with significant traffic and that support current cyber technologies to protect and defend ESINet and PSAP networks.

Interconnected Voice and Data networks could be a source of cyber threats to NG9-1-1 but, also a source of intelligence needed to gauge the size and potential impacts of an incident. NG9-1-1 gives citizens the ability to provide multimedia incident data such as voice, text, and imagery, although not all services will be available to all PSAPs. Some areas of possible investigation and development include the following:

a. Capabilities to analyze NG9-1-1 call data in near real time to insure valid information is presented to PSAP operators.
b. Capabilities to ensure content does not contain any malicious code that could damage or disable first responder networks.
c. Capabilities to ensure the content is valid and relevant to the incident that is presented to operators and responders.
d. Capabilities to consolidate and normalize data from the same or related incidents.
e. Capabilities to ensure content is not duplicative and does not contribute to information overload for PSAP operators and responders.

This project should explore developing a processing engine and algorithms for conducting near real time analysis of NG911-related content to analyze, classify, and filter via data mining to avoid overwhelming PSAP transport, hardware, software, CAD, and personnel resources. This should support the ability to geo-fence the incident more quickly and classify media as related to the primary or secondary event, avoiding duplication of effort. The project shall analyze geocode data from NG911 content to increase confidence in validity and location of an event to minimize malicious distributed attacks, Swatting, etc.

This project should also research leveraging AI/machine learning to more quickly contextualize public safety events and respond faster with the proper First Responder personnel. Other areas to consider include creating PSAP event/use case baseline for machine/AI-based learning via contextualizing/organizing existing electronic logged incident to determine classification parameters for each event. Determine the visual/audio/sensor-based information/parameters most common across similar events to allow AI to data-mine incoming ESINet NG911 media. For example, to determine active shooter event, what are the typical flags/identifiers (e.g. acoustic gunshot signatures)?

Research and identify methods of classifying and displaying near real time accuracies of location and time delay to continuously update areas of probability of 911/emergency caller location(s) from various geo-location sources and methods into E911 and NG9-1-1 proposed services.

This project shall research and identify processes to identify, detect, and mitigate the effects of integrity manipulation of perspective NG9-1-1 enterprise public safety video delivery services including: video altering, video time stamping, video authentication, video malware delivery attack and defense, video storage and retrieval services, and shared video distribution analysis services.

PHASE I:
Complete an overall examination of NG-9-1-1 architecture focusing on the threats and mitigations related to multimedia content originating from the public and propose how to better process, understand, and use this data in incident management. Propose how to develop and implement technologies to address these vulnerabilities, how to develop advanced data analysis capabilities as specified above, and how this can be done in a relevant operational environment suitable for piloting in partnership with DHS and other stakeholders the performer identifies and investigates.

Recommend a piloting environment, including participants and technologies to develop and deploy during Phase II. Develop a practical plan for technology development and implementation into a prototype and pilot.

PHASE II:
Develop and implement a prototype of the technologies defined in Phase I, in a relevant operational environment suitable for piloting in partnership with DHS Emergency Communications Division (ECD), DHS S&T, and other state or local government stakeholders. Lab testing should be conducted for the USG to verify the capabilities operate correctly, and then a pilot shall be conducted involving stakeholders, demonstrating and validating the concepts, technologies, and information sharing capabilities defined during Phase I.

Project plan and Systems Engineering deliverables such as design information, test plans, and test results should be included in the project. Provide recommendations on implementing the developed technologies in a large-scale deployment involving large, medium, and small ESINets and PSAPS.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS:
The technologies and methodologies developed in this SBIR will have possible wide-ranging application in the evolving NG9-1-1 landscape. NG9-1-1 will be replacing legacy E911 and 911 technology in the coming years. Funding opportunities will come from Federal NG9-1-1 grant programs to State and Local NG9-1-1

implementers. There will also be Federal NG9-1-1 implementations and organic State and Local funding.

REFERENCES:

FCC Task Force on Optimal Public Safety Answering Point Architecture (TFOPA) Working Group 1 Supplemental Report, 2016: https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG1_Supplemental_Report-120216.pdf

DHS Cyber Risks to Next Generation 9-1-1, November 2018: https://www.dhs.gov/sites/default/files/publications/NG911%20Cybersecurity%20Primer%20041216%20-%20508%20compliant.pdf

Next Generation 9-1-1 Cost Estimate: A report to Congress, 2018: Appendix A: NG9-1-1 Architecture, pages 69 – 161; https://www.911.gov/pdf/Next_Generation_911_Cost_Estimate_Report_to_Congress_2018.pdf

KEY WORDS: Next Generation 9-1-1, Cybersecurity, Task Force on the Optimal PSAP Architecture, Artificial Intelligence (AI), Analytics, Voiceover Internet Phone (VoIP), Session Initiation Protocol (SIP)

TECHNICAL POINT OF CONTACT: Dave Nolan, David.Nolan@cisa.dhs.gov

SBIR Topic Number: DHS201-002

TITLE: Remote Sensor Data Protection and Anti-Spoofing

TECHNOLOGY AREAS: *Data Protection, Remote Sensing, Bit Data, Machine Learning, Artificial Intelligence*

OBJECTIVE: Develop sensors or a sensor system capable of deployment in tactical, harsh, and rugged environments that are resistant to spoofing or data manipulation. Also required is a distributed sensor protection platform.

DESCRIPTION: Sensors of all types (e.g. range finders, thermal imaging devices, radar, ground sensors, radio frequency sensors, GPS, etc.) are actively being deployed to collect a wealth of data to inform critical law enforcement and intelligence missions. This data, while very valuable, is also at risk of manipulation, which can have adverse effects for these very same missions. There are multiple points of failure: the data being collected by sensors can be spoofed, resulting in false data being pushed upstream by an uncompromised sensor; alternatively, the sensor can be compromised, either physically or remotely, and false data can be generated by the sensor and then pushed upstream. This is especially of concern given that sensors tend to be the least-protected components of systems, as they are networked but often difficult to harden or physically protect.

There is an urgent need for a solution to be able to evaluate sensor data and prevent false data from being pushed upstream to operators, analysts and decision-makers. Furthermore, it is critical that this solution be deployable to tactical/harsh/rugged environments, so that data can be evaluated closer to the point of collection to avoid wasting critical bandwidth on bad or false data. Examples of such environments are at a US border, at a port, or on a shipping container.

The solution must:

1. Provide Multi-Domain Operation (MDO) capabilities required for data sharing and dissemination
2. Facilitate stateful inspection of sensor data, with a preference for remote inspection
3. Capability to process at least two data types, GPS sensor data and at least one other sensor data type. The ability to accommodate additional sensor data is preferred.
4. Evaluate valid sensor data packets and connections and detect anomalies
5. Provide a score for individual sensors, to identify sensors providing good or poor-quality data
6. Be customizable for edge devices
7. Quarantine bad/anomalous sensor data
8. Index and store qualified/standard sensor data

PHASE I: Proof of feasibility will include the delivery of reported spoofed sensor examples, spoofed sensor ingests, scanning and mitigation strategies, as well as scanning and mitigation interface design and description documents. The offerer will research and provide reported examples of at least two types of spoofed sensor data to include GPS, and the recommended mitigation strategies to be implemented in future research phases. As such, the offerer shall research, develop and document a minimum set of spoofing mitigation strategies to be implemented in future research phases. To demonstrate feasibility the offerer will provide these spoof and mitigation description documents as well as an interface design document for spoofed sensor data ingest filtering. This interface design document will include an example of a spoofed sensor data use case manually navigated through the ingest, filtering and mitigation process.

PHASE II: Develop, test and demonstrate a prototype based on the research and development conducted in Phase I. The prototype demonstration should simulate a tactical/harsh/rugged environment. The prototype must be tested to verify that it is resistant to spoofed data, and resistant to manipulated data. A relevant test

environment, as described, may be developed and used for the testing and demonstration, or a pre-existing test environment may be used.

At the conclusion of Phase II, the performer will conduct a technical demonstration of the prototype. In the technical demonstration, the contractor will demonstrate and validate the performance of the prototype. The demonstration and validation will include prototype resistance to spoofed sensor data, where sensors can be both physically and remotely compromised. Resistance to data manipulation will also be demonstrated and validated.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS:

Transitions is to Customs and Border Protection (CBP) for sensor monitoring along the US border, at ports, on shipping containers, or other rugged environments. There are potential DoD warfighter applications as well, depending on the particular sensor involved. For GPS sensors, if satellite navigation is not available, ground sensors may be used to identify relevant locations. The locations identified need to be accurately calculated from the sensor data, with confidence that the data has not been manipulated.

One potential commercial path is to guarantee that medical device sensor information has not been modified. This applies to implanted pacemakers or infusion pumps in particular.

REFERENCES:

1. *"A Machine Learning Approach for Detecting Spoofing Attacks in Wireless Sensor Networks";* Eliel Marlon de Lima Pinto; Rosana Lachowski ; Marcelo Eduardo Pellenz ; Manoel Camillo Penna ; Richard Demo Souza; IEEE; 2018. https://ieeexplore.ieee.org/document/8432315
2. "*GPS spoofing detection and mitigation using Cooperative Adaptive Cruise Control system*"; Nathaniel Carson ; Scott M. Martin ; Joshua Starling ; David M. Bevly; IEEE; 2016 https://ieeexplore.ieee.org/document/7535525
3. "*Effective GPS Spoofing Detection Utilizing Metrics from Commercial Receivers*"; Esteban Garbin Manfredini, Politecnico di Torino; Dennis M. Akos, University of Colorado at Boulder; Yu-Hsuan Chen, Sherman Lo, Todd Walter, Per Enge, Stanford Univeristy; 2018. https://web.stanford.edu/group/scpnt/gpslab/pubs/papers/GarbinManfredini_IONITM_2018_SpoofDetection.pdf
4. *"GPS Vulnerabilities for Critical Infrastructure"*, Department of Homeland Security, Science and Technology Directorate, 2016. https://www.dhs.gov/sites/default/files/publications/GPS%20Vulnerabilities%20for%20Critical%20Infrastructure%20Fact%20Sheet.pdf
5. *"This Ain't Your Dose: Sensor Spoofing Attack on Medical Infusion Pump"; Youngseok Park, Yunmok Son, Hocheol Shin, Dohyun Kim, and Yongdae Kim, Korea Advanced Institute of Science and Technology (KAIST); 2016.* https://www.usenix.org/conference/woot16/workshop-program/presentation/park

KEY WORDS: Distributed sensor system, sensor system integrity, manipulation of sensor data, GPS data manipulation, sensor spoofing, data spoofing

TECHNICAL POINT OF CONTACT: Ann Cox Ann.Cox@hq.dhs.gov

SBIR Topic Number: DHS201-003

TITLE: Digital Paging over Public Television

TECHNOLOGY AREAS: *Interoperable Communications and Data Program, Community and Infrastructure Resiliency Program*

OBJECTIVE: Define and demonstrate a secure, standards-based, public safety one-way digital paging system for daily and disaster uses.

DESCRIPTION:

Fire and EMS services across the United States still rely on analog voice pagers to communicate emergency incident information. The infrastructure for these paging systems is typically operated by the local agency providing coverage to that geographic jurisdiction. The limited coverage does not provide notification to individuals that have traveled outside of the area, for work or vacation. It also creates a silo and information is not shared outside the coverage area. This voice pager is also based on technology that is slow at delivering emergency information as it takes time for a dispatcher to read the information. This type of pager uses a "selective call" feature to keep the pager silent until the pager's programmed code or tone is detected. Each unique tone can be 2-3 seconds long and when multiple tones need to be sent, all the tones must be transmitted sequentially before any of the dispatch information can be delivered. Then, the actual voice dispatch can take 20-40 seconds depending on how much verbal information is provided. During all of this, other emergencies are queued waiting for the paging transmitter to become available.

Today's digital television uses the Advanced Television Systems Committee (ATSC) standard, also known as ATSC 1.0. ATSC 1.0 is used to broadcast many other types of useful information besides video, such as TV program guides, emergency alerts, etc. An enhancement to the current ATSC 1.0 digital broadcast system, known as ATSC 3.0, is now being deployed. ATSC 3.0 utilizes a different delivery scheme that is far more robust and useful for mobile applications. It also has the added benefit of better building penetration and is four times more efficient than the current system. The increased bandwidth will be available for non-video applications.

ATSC 3.0 may present the perfect opportunity to research a solution for the current challenges found with existing analog voice paging (speed, coverage, silo, and capacity). An ATSC 3.0 solution could provide such robust coverage to reach an entire state's geography, including tribal lands and rural areas utilizing existing infrastructure.

Such a solution has not been tried in the past as ATSC 1.0 is not designed for reception from a moving receiver, as needed by a volunteer firefighter driving down the road would be wearing.

The requirements for this solution include:

- Establish a direct connection with the Public Safety Answering Point (PSAP, aka 911 Center) that does not rely on the public internet for relay of dispatch information
- Creation of a centralized server to process emergency dispatch information from various PSAPs to be injected into the ATSC 3.0 broadcast stream
- Develop an ATSC 3.0 receiver that would decode the emergency dispatch information
- Allow the receiver to determine the alert trigger (programming should be maintained at the receiver level to mimic today's analog pagers)
- Based on standards to allow multiple receiver manufacturers

- Receiver could utilize a smartphone to achieve the following features or such features would need to exist on a portable stand-alone device:
  - Receiver should have a battery life of at least 18 hours
  - Receiver should have a low battery alarm
  - Receiver should support a text to speech function
  - Receiver should have a display
  - Additional requirements found in National Fire Protection Association (NFPA) Handbook 1221

PHASE I:

Prove feasibility of propose approach to include the following:

- A defined data standard used to export emergency dispatch information coming from the PSAPs Computer Aided Dispatch (CAD) software.

- A design and development plan for a paging server that would collect and conform the dispatch information into a common protocol that would then be delivered to the ATSC 3.0 enabled transmission system. Such information will include event type (fire, car crash, stroke, etc.), event location, units dispatched, etc.), and the date and time of dispatch, among other fields.

PHASE II:

By the end of Phase II, the performer shall provide:

- A demonstration of a prototype of an ATSC 3.0 paging receiver that displays the CAD information sent from the paging server to the ATSC 3.0 transmitter.

- Results from research of the ATSC 3.0 delivery chain to explore various configurations that optimizes delivery to the paging receiver without compromising the Public Broadcasters FCC requirement for television program delivery.

- Results from performance modeling and testing of ATSC 3.0 receptibility in a controlled environment for anticipated paging receiver design (for example, body worn small device on a belt).

- Prototype two different paging receiver designs, one based on a stand-alone model and the other based on a smartphone integration with the ATSC 3.0 information passed along to a smartphone application. Provide a practical demonstration of the capability with at least 10 receivers located with different first responder organizations from different jurisdictions within a state. The organizations should represent different types of jurisdictions from urban to rural, career to volunteer, mountainous to coastal.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS:

Phase III will involve the productization of the server and receiver designs, resulting in the validation of the paging server by connecting to several PSAPs in operation and finalize any field mapping or other challenges presented by multiple CAD vendors, and developing a scalable process for the centralized paging server to receive data from new CAD vendors or versions that have not been encountered prior.

The technology could be developed into a business model that would allow the local public television station to partner on a bid for replacement of a local first responder agencies' current paging system. This technology will need to be evaluated by the NFPA and/or ISO Mitigation (VeriRisk) to gain acceptance as a dispatch

technology used by the fire service. This concept can easily be expanded to other areas and use cases for one-way directed paging such as law enforcement agencies, search and rescue teams, government leadership, federal responders, etc. Partnering with PBS could lead to a nationwide public safety paging system that could be utilized by FEMA, the National Guard, and other federal assets. ATSC 3.0 can also represent a delivery method for public notification of weather events or disaster, possibly even replacing the National Oceanic and Atmospheric Administration's (NOAA) Weather Radio All Hazards (NWR) network of 1000+ radio stations.

REFERENCES:

1. NFPA 1221 Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems. (2019)https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1221

2. ATSC 3.0 Standards https://www.atsc.org/standards/atsc-3-0-standards/

KEY WORDS:
Communications, Paging, Datacasting, ATSC 3.0, Dispatch, Alerting, Emergency Communications, Fire Station Alerting

TECHNICAL POINT OF CONTACT: Denis Gusty, Denis.Gusty@hq.dhs.gov

SBIR Topic Number: DHS201-004

TITLE: Soft Targets and Crowded Places Security

TECHNOLOGY AREAS: *Soft Target Security, Emerging and Evolving Threats, Active Assailant Attacks, Improvised Explosive Device, Firearms, Unmanned Aircraft Systems, Vehicles Ramming, Security Screening, Mass Gatherings, Special Events, Mobile Technology, Artificial Intelligence, Augmented Reality*

OBJECTIVE: Develop a capability to identify and mitigate threats toward reducing the overall risk to soft targets and crowded places.

DESCRIPTION:
Soft targets and crowded places continue to be attractive targets for violent extremists determined to inflict harm and disrupt the American way of life. As such, protecting these inherently vulnerable locations has become a National imperative and priority for DHS. "As the DHS lead for the soft targets and crowded places security effort, Cybersecurity and Infrastructure Agency (CISA) supports partners to identify, develop, and implement innovative and scalable measures to mitigate risks to these venues; many of which serve an integral role in the country's economy" (*Page 8, CISA Strategic Intent, 2019).* To support these efforts, CISA Infrastructure Security Division (ISD) has made mitigating threats to soft targets and crowded places its top priority (*CISA Security of Soft Targets and Crowded Places- Resource Guide, February 2019*).

CISA ISD is actively engaged with public and private sector partners to enhance their security and preparedness through awareness and training. However, protecting soft targets and crowded places against future active assailant attacks requires a more comprehensive approach that includes advanced technology. Development of a capability to identify and mitigate risks to soft targets, with the ultimate goal of incorporating an augmented reality platform applications is needed. Such a technology would enable security professionals to view their environment through a mobile device while applying augmented reality and artificial intelligence to consider the advantages and disadvantages of various mitigation methods against known threats.

PHASE I:
Phase I will include a proof of concept with an incremental approach to ensure proper applicability, including:

- Planning to identify and acquire sourcing material information
- Identifying initial risk indicators
- Scaling and surveying landscapes and environments
- Developing an initial methodology and assessing the potential effectiveness of the approach.

PHASE II:
Phase II will focus on executing the Phase I project plan. This will include:

- Continuing methodology development toward identifying key aspects of soft target risk assessment and mitigation techniques
- Surveying and designing environmental layering
- Injecting threat vectors into artificial intelligence
- Assessing the approach in a set of relevant scenarios
- Organizing design elements and data toward future implementation of an augmented reality capability

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS:
Development of technology building off of the findings from Phase II. This technology will be developed for use by both private sector, and government applications, but in an iterative order, pending success and lessons learned of the GOTS application, then deployment to COTS.

The government applications will be leveraged by federal and contract staff to use in both headquarters and field assessments, planning, and special events security coordination. For example, prior to a special event, a Protective Security Advisory or other field staff could deploy this technology to conduct a security assessment of a facility, enabling the assessment team to visualize placements of certain security features or physical measures.

The private sector or commercial use of this technology is intended to be leverage directly by security managers, event planners, owners/operators of critical infrastructure, and other private entities that have equities in security of soft targets. This commercial application will be off-the-shelf and available for entities to use not necessarily requiring government oversight or assistance.

REFERENCES:

1. DHS Soft Targets and Crowded Places Security Plan Overview (https://www.dhs.gov/publication/securing-soft-targets-and-crowded-places-resources)

2. CISA Strategic Intent- Defend Today, Secure Tomorrow- 2019 (https://www.dhs.gov/publication/cisa-strategic-intent)

3. CISA Security of Soft Targets and Crowded Places- Resource Guide - AD Harrell welcome letter (https://www.dhs.gov/sites/default/files/publications/19_0424_cisa_soft-targets-and-crowded-places-resource-guide.pdf)

KEY WORDS: Soft Targets, Crowded Places, Active Shooter, Vehicle Ramming, Unmanned Aircraft Systems

TECHNICAL POINT OF CONTACT: Josha Jordan, Josha.Jordan@cisa.dhs.gov

SBIR Topic Number: DHS201-005

TITLE: In-building Coverage Analysis System (ICAS) Using Existing First Responder's Radio and Smartphone.

TECHNOLOGY AREAS: I*nteroperable Communications and Data Program, In-building Public Safety Communications, Public Safety Land Mobile Radio and Broadband Communications, FirstNet.*

OBJECTIVE: Develop a capability to acquire and document network signals inside of buildings for public safety land-mobile radio (LMR) and the FirstNet broadband network to inform public safety users about wireless service availability in designated buildings and to plan for in-building coverage enhancement solutions.

DESCRIPTION: First Responders must maintain access to communications tools at all times – yet, in many instances, this access is hampered due to partial and/or total attenuation of the communication signals inside of a building, making it difficult for first responders to maintain proper situational awareness during dangerous indoor operations. First Responders must rely on their agency's LMR radios as the primary means for voice communications in indoor settings. At the same time, the availability of FirstNet LTE network is increasingly providing additional indoor data services such as physiological and health monitoring and location tracking to enhance personnel safety. However, the LMR and FirstNet networks are two completely separate networks, and more importantly, neither of these networks currently afford reliable in-building network coverage levels as mandated by the National Fire Protection Association (NFPA) or the International Fire Code (IFC). In short, there is a need to allow first responders to record, access and update the in-building service availability of each of these two different networks for the next ten years or even longer.

Existing systems and methods allow for the characterization of indoor service availability for either LMR or FirstNet individually, but not both at the same time. Commercially-available tools and/or solution do not provide a side-be-side comparison of the service availability of both LMR and FirstNet networks, and each network is expected to play crucial roles in supporting public safety users in the foreseeable future for interoperable voice and data communications.

There exists a need for a system and method to:

1) Simultaneously measure and map LMR and FirstNet network's service availability inside of vital and institutional buildings (such as underground subway stations, and airport);
2) Interface with existing first responder's radio and LTE devices to ensure the results reflect what the responders will experience while operating indoor; alternatively, if the measurement devices do not utilize existing first responder's prevailing devices, then the proposed user device(s) (e.g., software-defined radio) must produce measured results which align with typical end-user devices (LMR radios and LTE smartphones) 90% of the time in at least 5 buildings designated as "vital" by DHS in a given locality (e.g., airport, subway station, or a large mall or an apartment complex);
3) Establish a portable software application to allow public safety or third-party personnel to plan and carry out in-building coverage test and upload the data to a central database;
4) Develop a user interface to view the central database to give first responders the ability to perform side-by-side comparison of the in-building coverage, help inform and improve any potential indoor coverage service gaps for both LMR and FirstNet;
5) Equip the central database to ingest and archive test results measured at different times/dates for a same building to enable the viewing of historical coverage test results;
6) Devise in-building test method and system verification and conform with grid-based coverage test procedures – refer to National Fire Protection Association (NFPA-72-2010) or International Fire Code (IFC 2012) guidelines (reference document is provided).

Any identified indoor coverage gaps will further inform any remedial actions such as distributed antenna systems (DAS), radio repeaters, or similar technologies to further improve indoor coverage to meet appropriate locally-mandated laws and regulation.

Additionally, a robust in-building coverage assessment program serves to address indoor personnel geolocation capability needs as described by the DHS S&T Project Responder 5 Capability Need report, also known as the PR5 report.

PHASE I: Conduct a complete feasibility analysis of the requirements outlined above and develop a framework for the operating components of the ICAS. A report must be accompanied by a sample test report conducted by the offeror for three sample 10-15-story buildings depicting the side-by-side coverage of the LMR vs. FirstNet coverage.

PHASE II: Develop ten ICAS prototypes providing fully integrated hardware and software components to address the in-building coverage acquisition requirements outlined in this request. Tools and functionalities shall encompass:

1. Develop an integrated ICAS measurement tool and process for a single end-user to hand-carry on commercial tablet or hand-held devices for the purpose of measuring and storing in-building network coverage information;
2. Provide interface to obtain network coverage data for up to three commercial LMR radio models and three smartphone models;
3. Define measurement process in accordance with industry-accepted procedures – NFPA-72-2010 and IFC document for public safety communications shall be used as guidelines;
4. User-definable indoor maps to display the coverage data;
5. User-definable coverage thresholds (in dBm) to depict network coverage;
6. User interface to allow user to query a central coverage database for historical test results for a given building; at a minimum, such query must provide a visual coverage results (heat maps) for each floor where test results were collected; at a minimum, such query must provide quantitative comparison between two different test runs on a) per floor basis, and b) on a per building basis;
7. Provide a scalable coverage database to accommodate test results for a minimum of 1,000 buildings (and scalable to 10,000 buildings in the future if required) and store least five distinct test results per building;

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS:

Further development shall be required in Phase III to support both Homeland Security and commercial applications, and shall include:

1. Complete documentation required to operate the ICAS tool;
2. Certify the ICAS measurement application for use on both iOS and Android mobile devices;
3. Provide ICAS tool updates and maintenance for a period of 24 months following the completion of the project;
4. Provide up to five 1-day user training sessions on the operation of the ICAS.

Homeland Security Application: ICAS can be used by DHS Component users to conduct in-building coverage at key installations such as airports, ports-of-entry, border crossings, and Coast Guard maritime assets.

Commercial Application: ICAS can be used by state, local, and tribal public safety agencies, as well as by commercial cellular carrier personnel to conduct in-building test to fully characterize the service availability of LMR and FirstNet network coverage.

REFERENCES:

1. "Public Safety Radio Indoor Coverage Systems – Rules and Regulations", Publicsafetydas.org; http://fuzewireless.com/wp-content/uploads/2015/02/publicsafetymandates1.pdf
2. The NFPA-72 National Fire Alarm and Signaling Code, http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=72
3. The International Fire Code (IFC) section 510, available at https://www.diversifiedelectronics.com/ifc-510-testing/
4. 700 MHz In-Building Coverage App & Measurement System Development, National Institute of Science and Technology (NIST) Public Safety Communications Research (PSCR) program, https://www.nist.gov/programs-projects/700-mhz-building-coverage-app-measurement-system-development
5. Project Responder 5 Final Report, https://www.dhs.gov/sites/default/files/publications/Project-Responder-5-Report_170814-508.pdf, DHS S&T FRRG

KEY WORDS: public safety broadband communications, in-building wireless coverage, land-mobile radio, mission-critical communications services, 3GPP networking standards, 4G and 5G services, FirstNet, resilient communications networks.

TECHNICAL POINT OF CONTACT: Cuong Luu, Cuong.Luu@hq.dhs.gov

SBIR Topic Number: DHS201-006

TITLE: Handheld Advanced Detection/Imaging Technology System

TECHNOLOGY AREAS: *Aviation Security, Passenger Screening, Alarm Resolution, Radar*

OBJECTIVE: Develop a handheld passenger screening device capable of detecting prohibited items relevant to aviation security.

DESCRIPTION:
Currently fielded aviation passenger screening systems are large, fixed systems capable of detecting concealed objects on a person. While this approach is useful for standard passenger screening, there are additional requirements for a handheld system to enable concepts of operations that the fixed systems cannot accommodate. These include:

- Pop-up checkpoint environments suitable for employee screening or other random supplemental security measures
- Alarm resolution procedures where additional inspection is required but may prevent a physical pat-down
- Locations that cannot accommodate a fixed system due to size, weight, power, or cost limitations

Key requirements of a proposed solution must include:

- Active illumination with non-ionizing radiation
- Ability to compensate for intentional (deliberate sweeps) or unintentional (shaking) motion of the handheld device
- Ability to run automated detection algorithms to distinguish between a concealed object and clothing/skin while respecting privacy
- Low-power, able to run from a battery for 3-4 hours without recharging
- Low-cost, targeted volume cost of $5,000 or less

Previous systems have tended to be passive systems that lacked the resolution to detect more complex threats at a reasonable price point. However, recent developments in low cost components for 5G wireless networks and associated handheld electronics may allow for solutions that meet performance, size, weight, power, and cost requirements.

PHASE I:
Develop requirements and a system concept backed by sufficient modeling and simulation to determine technical feasibility of the proposed approach. The final technical report shall include performance specifications, design feasibility, and a draft test and evaluation plan for evaluating system performance against the defined requirements.

PHASE II:
Complete detailed design, fabrication, and testing of initial handheld screening prototypes. If testing results show that the system meets the system requirements defined in the description, Phase II may include an operational evaluation in a laboratory and/or operational test environment. The Phase II deliverables include three prototype units and relevant testing in accordance with the test and evaluation plan defined in Phase I.

PHASE III - COMMERCIAL OR GOVERNMENT APPLICATIONS:
Phase III includes additional design for manufacturing efforts to adapt the prototypes developed in Phase II to full volume production. Depending on the design, Phase III may also include certification and qualification of

the system against relevant Transportation Security Administration (TSA) standards. Potential applications of the technology include TSA deployment at the aviation checkpoint or for employee screening but could also be deployed by the private sector for screening at sporting events, concerts, or other secure areas.

REFERENCES:

Aviation Security Advisory Committee, "FINAL REPORT OF THE AVIATION SECURITY ADVISORY COMMITTEE'SWORKING GROUP ON AIRPORT ACCESS CONTROL", https://www.tsa.gov/sites/default/files/asac-employee-screening-working-group-04-15.pdf

National Academies of Sciences, Engineering, and Medicine. 2017. "Airport Passenger Screening Using Millimeter Wave Machines: Compliance with Guidelines (Chapter 2)". Washington, DC: The National Academies Press. https://doi.org/10.17226/24936.

Microwave Journal, August 2007, "The Next Wireless Wave is a Millimeter Wave" https://pdfs.semanticscholar.org/435a/ba0e91b60fbbd5a12f7ee390491953c2f898.pdf

MDPI, "Survey of Motion Tracking Methods Based on Inertial Sensors: A Focus on Upper Limb Human Motion" https://www.mdpi.com/1424-8220/17/6/1257

KEY WORDS: Passenger Screening, Radar, Explosives Detection, Inertial Measurement Unit, Automatic Threat Recognition, Low-Cost, Sensor

TECHNICAL POINT OF CONTACT: Dr. John Fortune, john.fortune@hq.dhs.gov

SBIR Topic Number: DHS201-007

TITLE: Enhanced Explosives and Illicit Drugs Detection by Targeted Interrogation of Surfaces

TECHNOLOGY AREAS: *Explosives and illicit drugs detection, non-contact sampling, Screening at speed, Alarm Resolution, Trace*

OBJECTIVE: Develop quick and efficient targeted surface interrogation technique(s) by locating and detecting trace residues of interest on carry-on baggage and items.

DESCRIPTION: Screening, detection, and identification of explosives and illicit drugs at aviation checkpoints, border crossings, and U.S. ports of entry play a critical role in supporting mission spaces of the Homeland Security Enterprise, especially that of DHS Transportation Security Administration (TSA) and Customs and Border Protection (CBP). Since 9/11, TSA has employed contact and non-contact sampling of personnel and baggage in conjunction with Ion Mobility Spectrometry (IMS) as a standard explosives trace detection tool to maintain safety in air transportation environments. CBP employed chemical identification equipment such as IMS, Raman and Fourier Transformed Infrared spectroscopy at U.S. ports of entry and U.S. Border Patrol checkpoints to detect and identify illicit drugs. These detectors are employed as part of a multi-layered, risk-based approach to combat the flow of illicit drugs especially that of emergent and dangerous synthetic opioids.

In all aforementioned operational environments, sampling is a critical step in enhancing sensitivity of explosives and illicit drugs detectors. The more sample is delivered to a detector's sampling inlet, the more sensitive the detection.

Targeted interrogation of surfaces would enhance non-contact explosives and illicit drugs detection technologies by directing these modalities toward surfaces that have residues of interest for interrogation. This would increase the amount of sample to be collected and ultimately detection sensitivity.

In order to meet screening at speed requirements and enable targeted interrogation, DHS S&T is looking for a solution that can:

1) Locate trace residues and particles within a few seconds on surfaces of various carry-on items such as luggage, laptops, and others.
2) Communicate with trace detection modalities on the locations of the trace residues and particles.
3) Integrate with trace detectors including, but not limited to, optical techniques, vapor jets that dislodge particles, vacuum-type of samplers, and IMS.
4) Potentially integrate with TSA and CBP in-line carry-on baggage screeners.

PHASE I: Conceptualize, design, and develop a proof of concept for an innovative solution to detect, locate, and determine range (range finding) of trace residues and particles of interest. The residues are sub-microgram amounts of materials of interest imprinted on carry-on items such as bags, laptops, and other items. This phase will provide proof that the proposed concept can accomplish the detection, location, and range finding of the residues of interest within two seconds from start to end of the scanning sequence.

PHASE II: Develop, deliver, and demonstrate two prototypes of the proposed design in Phase I that successfully locate trace particle of interest on luggage and laptops. Trace residues are imprinted on five different surface substrates to be communicated by the Government. The prototype demonstration should include the ability to communicate with trace detection modalities on the locations and ranges of the trace

residues and particles, and be integration ready with trace detectors. The solution could include both software and hardware into a low-cost prototype of less than $20,000. Size and weight is negotiable, but the prototypes are expected to be the size of a shoe-box.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS:
Up to three prototypes are expected to be further developed to send to an independent laboratory for technical assessment. The proposer will work with the government to determine realistic testing and assessment scenarios to include an expanded list of surfaces that can be sampled. The government will also work with the performer to identify and execute additional field assessment opportunities with end-users to provide feedback. Results from these assessments are expected to be incorporated into further refinement of the prototypes which shall then be ready for integration into systems ready for Test & Evaluation by a government laboratory. A successful solution will produce a quick and efficient way to find trace particles in Homeland Security environments such as airports, ports of entry, and other screening venues.

REFERENCES:

- https://www.dhs.gov/science-and-technology/apex-screening-speed
- https://www.tsa.gov/sites/default/files/resources/technology_factsheet.pdf
- https://www.dhs.gov/science-and-technology/secondary-screening
- https://www.tsa.gov/videos/inside-look-inline-baggage-screening-systems-0

KEY WORDS: Explosives and illicit drugs detection, standoff detection, alarm resolution, trace, non-contact sampling, targeted interrogation of surfaces, screening at speed, checkpoint, checked baggage

TECHNICAL POINT OF CONTACT: Laura Parker, laura.parker@hq.dhs.gov

SBIR Topic Number: DHS201-008

TITLE: Urban Canyon Detection Tracking and Identification of Small Unmanned Aerial Vehicles

TECHNOLOGY AREAS: *Air Domain Awareness, ADA, Counter Unmanned Aerial System , UAV, Covered Assets, Critical Infrastructures, Acoustic Sensors, Radio Frequency Sensors, Light Detection and Ranging*

OBJECTIVE: Demonstrate the ability to detect, track, and identify small (55 pounds or less including payload but could be up to 100 pounds for some systems) unmanned aircraft vehicles (UAV) in an urban canyon environment.

DESCRIPTION: The commercial use of unmanned aerial systems (UAS) in urban environments for applications such as package deliveries and surveying are expected to start soon. Nefarious uses of UAS in the urban environment will follow. Current technology for UAV detection, tracking, and identification is problematic. The detection and tracking of UAVs (both singular and swarms) is a critical task complicated by low flight height, small radar cross sections, and a complex background that include birds, insects, and flying debris. The problems for this task increase further with complex structures and high buildings that form urban canyons that block lines of sight.

Urban canyons are characterized by dense and uneven clutter, strong multipath, and limited line-of-sight. In addition, targets can perform evasive maneuvers or undergo a track swap owing to congested environments. Urban canyons can be described by their geometric aspect ratio - the ratio of the sum of the average building height on either side of street divided by street width. A deep urban canyon will have a ratio of >2.

To fill this capability gap DHS needs a blend of detection and tracking technologies that can both discriminate different kinds of UAVs and identify nefarious UAVs, while subtracting out the other kinds of nuisance urban air traffic. These technologies have to perform in concert within tactical timelines envisioned for nefarious mitigation (tens of seconds).

Current systems enjoy uninterrupted lines of sight, elevated pointing angles, and have intended targets with ample radar cross sections and consistent visual profiles.

Demonstrate a small UAV detection, tracking, and identification sensor system that:

- Discriminates small UAS from common urban chaff such as birds, insects, and other flying debris,
- Performs discrimination and tracking concurrently against multiple air targets of interest,
- Performs within timelines useful for completing a fire control loop needed for mitigating nefarious UAVs,
- Operates in a complex urban radio frequency and acoustic environment,
- Performs at night and in weather consistent with small UAV capabilities,
- Can be safely operated in the presence of human beings down range without biological damage (e.g., retina damage from laser light),
- Meets FCC and FAA requirements for use in urban environments.

PHASE I:

Provide a small UAV urban canyon sensor concept feasibility design described in a Phase I technical report. This description shall contain a concept viability analysis with expected performance. Aspects that should be considered for a small UAV detection, tracking, and identification sensor in the hardware, electrical and software feasibility design include:

- Discriminating small UAS from common urban chaff such as birds, insects, and other flying debris,
- Performing tracking concurrently against multiple air targets of interest,

- Completing a fire control loop timeline needed for mitigating nefarious UAVs
- Operating in a complex urban radio frequency and acoustic environment,
- Addressing night and weather environments consistent with small UAV capabilities,
- Can be safely operated in the presence of human beings down range without biological damage (e.g., retina damage from laser light),
- Complying with FCC and FAA requirements for use in urban environments.

Activities in the Phase I produces artifacts addressing the following areas;

- Sensor concept feasibility descriptions,
- Intended software architecture,
- Notional electrical architecture,
- Envisioned hardware layout.

There shall be an urban canyon sensor concept feasibility design report that incorporates the above.

PHASE II:
Complete the design of the demonstration sensor system, deliver a system for a demonstration, and conduct a demonstration of the system. Development of the Phase II demonstration prototype design produces artifacts that address the following areas;

- Software module descriptions,
- Electronics and power distribution,
- Final packaging layout,
- Other items such as specifications, cut-sheets, drawings, schematics, software artifacts (including source code) and all other documents developed under the effort.

Full operation of system capacities may be demonstrated in an operational environment that is yet to be determined. There shall be a demonstration technical report on design and demonstration of system.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS:

Successful completion of Phase II will allow for evaluation of the sensor system for future enhancements. Locations envisioned for the operational capability could include; airports, critical infrastructure, U.S. borders and events designated with a Special Event Assessment Rating of 1 or 2.

REFERENCES:

1. https://uasmitigationatairports.org/blue-ribbon-task-force-on-uas-mitigation-at-airports-interim-report/
2. https://www.srcinc.com/pdf/Whitepaper-Countering-the-CUAS-shortcomings.pdf
3. https://fas.org/irp/doddir/army/atp3-01-81.pdf
4. https://dronecenter.bard.edu/files/2018/02/CSD-Counter-Drone-Systems-Report.pdf
5. https://jrupprechtlaw.com/drone-jammer-gun-defender-legal-problems/

KEY WORDS: Counter unmanned aircraft system (CUAS), air domain awareness (ADA), unmanned aircraft system (UAS), unmanned aircraft vehicle (UAV), SUAS,

TECHNICAL POINT OF CONTACT: Jeffrey Randorf, jeffrey.randorf@hq.dhs.gov

SBIR Topic Number: DHS201-009

TITLE: Machine Learning Module for Detection Technologies

TECHNOLOGY AREAS: *Standoff detection, Screening at Speed, Optical Trace, Secondary Screening*

OBJECTIVE: Develop a standard compact high-performance software and/or hardware module that rapidly classifies unknown spectra as safe or a threat.

DESCRIPTION:
The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) is looking towards next generation technologies that provide non-contact, inexpensive, quick, and accurate detection of explosive threats. DHS S&T is researching, developing, and evaluating optical technologies as part of this effort with the potential to be used across multiple Concepts of Operations (CONOPs) in the DHS enterprise. Through DHS S&T, sophisticated spectrometer systems, apparatuses used for recording and measuring spectra, have been built and designed to deliver a signal that can then be fed to an algorithm for "threat" detection. Each system and vendor take their own approach to the algorithm, at significant cost to the vendor and DHS S&T, and with highly variable results. Offering a standard machine learning (ML) platform would expedite the algorithm component of programs, allowing more resources to be dedicated to hardware development.

While machine learning can take many forms, numerous successful, convolutional neural network (CNN) routines, such as Alexnet or Googlenet, follow a similar "image recognition" paradigm. Such routines are ubiquitous and are freely available for download in the internet. They have been developed over many years to identify objects (such as cats, dogs, faces, cars, etc.) and have converged toward very high success rates in open competitions. Applying these algorithms to signals such as the output of spectrometers offers a rapid development path. What is required is a standard executable user interface that can accept training data, convert it to a format compatible with the CNN (such as a JPG image), and then return a classification (detection) value for an "unknown" signal.

In addition, large desktops and laptop computers are used for data processing for most projects. This is despite the promise of building compact advanced feasibility demonstrators (AFD) or prototypes. Ultimately, this processing capability needs to be available to the portable system in near real time. Developments in Graphical Processing Units (GPU) can offer high performance in a compact platform. Because ML algorithms are computationally intensive, the board level processor running the user interface must have high performance. Although CNN networks may require many hours of training on large data sets, once trained, they can perform detection or classification tasks in milliseconds. Because the trained CNNs are typically just a small file, they offer the opportunity for the fielded "testing" processor to require only a fraction of the computational power of the laboratory "training" processor.

Being able to offer a standard compact high-performance software and/or hardware machine learning algorithm platform would dramatically accelerate technology development and ultimately save DHS the cost of redundancy.

PHASE I - SOFTWARE DEVELOPMENT AND HARDWARE DESIGN:
Demonstrate proof of concept of proposed interface for classifying spectrometer signals for standardizing a machine learning algorithm. Determine feasibility of generalizing the parameters required to input spectrometer data into a CNN. This includes standardizing the input properties of the training data set, as well as the output properties of the classifier algorithm.

The end user will deliver a preliminary software interface document describing the format and requirements for

all data inputs such as training and unknowns. This document will also describe the user interface and format for the data outputs. If applicable, a preliminary hardware design document shall be included, specifying the components to be used, their expected performance, cost, size, weight, and power consumption.

PHASE II - PROTOTYPE DELIVERY AND TESTING:
Build, deliver, and test two prototypes that include sufficient processing power to run the machine learning algorithm for training and classification. Prototypes will be tested against relevant data sets. Prototype performance metrics include training time, the time to return an output (detection) value, the accuracy, false alarm rate, and receiver operating characteristic (ROC). If applicable, prototype hardware design should be a shoebox size, weigh no more than 50 lbs., and balance power consumption with performance. It is acceptable, even preferred, for hardware to include two separate processor units, a larger stand-alone box for training on large data sets and a much smaller "testing" processor capable of classifying individual unknown spectra.

PHASE III - COMMERCIAL OR GOVERNMENT APPLICATIONS:
Applications for the Machine Learning Module can include both government and commercial programs. DHS S&T could offer replicates of the Module directly to selected technical performers or to commercial vendors. The Module is designed to serve two functions for DHS. The first is to expedite algorithm development for performers developing spectroscopic (ion mobility, Raman, Infrared, mass spectrometry, etc.) technologies. This reduces risk, increases return on investment, and reduces redundancy across performers. The second benefit is to offer a compact fieldable module compatible with prototype spectroscopic systems, thereby enabling them as "detectors" of threats such as explosives, chemical agents, and drugs of abuse based on pre-trained "library" spectra. This expedites the advancements of technology into fieldable systems, increasing the pace and likelihood that they can be delivered to end users. Numerous DHS programs, such as Next Generation Explosive Trace Detector (ETD) and Apex Screening at Speed (SaS), would benefit from access to such a Module. In addition, any vendor developing spectroscopic technology for the Homeland Security market, would benefit from utilizing the Module as part of their process.

REFERENCES:

1. Alexnet Convolutional Neural Network: https://neurohive.io/en/popular-networks/alexnet-imagenet-classification-with-deep-convolutional-neural-networks/
2. Googlenet Convolutional Neural Network: https://ai.google/research/pubs/pub43022
3. "Active LWIR hyperspectral imaging and algorithms for rapid standoff trace chemical identification," Proc. SPIE 10986, Algorithms, Technologies, and Applications for Multispectral and Hyperspectral Imagery XXV, 109860K (14 May 2019); doi: 10.1117/12.2518720
4. Receiver Operating Curve: https://www.statisticshowto.datasciencecentral.com/receiver-operating-characteristic-roc-curve/

KEY WORDS: Machine learning, Algorithm, Prototype, User interface. Neural network, Spectroscopy, Detection

TECHNICAL POINT OF CONTACT: Mike Palamar, michael.palamar@hq.dhs.gov

SBIR TOPIC NUMBER: DHS201-010

TITLE: Innovative Technologies for Next Generation of Sample Collection Media

TECHNOLOGY AREAS: Biological Hazard Containment, Reduce Contamination Hazards, Mission Oriented Protective Posture (MOPP), Reduced Life Cycle Costs and Logistical Burdens

OBJECTIVE: Survey and identify current commercially available air sampling collection media. Develop novel or improved air sampling collection media for biological hazards.

DESCRIPTION: Ambient air sampling methods are important for determining the quantity or quality of pollutants in the air or environment. Certain air sampling media are design to collect biological hazards to be extracted for future testing[1]. The Department of Homeland Security (DHS) Countering Weapons of Mass Destruction (CWMD) Office is pursuing development of reliable, cost-effective, validated and sustainable collection media either dry or wet sample collection media that can collect and store the bio threat particles for 24 to 36 hours and allow the viable extraction of the DNA from the threat particles. The ability to collect and extract small quantities of biological materials is of particular interest. The air sampling media must be able to:

1. Maintain a viable biological sample up 24 hours of intake of ambient air flow.
2. Collect and maintain a viable biological sample at air intake rates of 100-1000 liters per minute.
3. Move media from collection site to laboratory testing site without loss of sample.
4. Allow extraction of collected sample from media up to 48 hours after media is removed from collection device.

PHASE I: Identify novel and improved approaches to collection media that allow extended media sample storage and extraction of viable biological materials compared to currently available technology. This includes the following:

- Identification of current ambient air sampling technologies.
- Performance and limits of current technologies.
- Approach to improve current technologies to increase viability of biological sample.
- Development of novel air sampling technologies as compared to current technologies.

Phase I deliverables include monthly progress reports and a final Phase I report addressing the items above. Project review meetings will be held at the initiation, mid-point and completion of the Phase I effort.

PHASE II: This phase will expand on Phase I, conducting the actual research and development to enhance the performance of current technologies. Phase II will also produce novel air sampling media that outperforms current commercially available media that will include the following:

- Increased biological sample concentration and viability after up to 24 hours of air flow at 100-1000 liters per minute.
- Reduced loss of biological sample concentration after removal of media from collection device.
- Increased viability of biological sample 24-48 hours after media is removed from collection device.

Phase II deliverables include monthly progress reports and annual technical reports. At least one improved prototype and one novel prototype will be delivered to CWMD (or its partners, as directed) at the end of Phase II. Project review meetings will be held throughout the project period as needed to include but not limited to the initiation, mid-point and completion of the Phase II effort.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: Phase III activities would include a successful commercialization strategy for supporting the integration of improved or novel technologies into the current or emerging CWMD biological detection and identification efforts.

REFERENCES:

1. Detecting Bioterrorist Attacks. (https://www.dhs.gov/biowatch-program)

KEY WORDS: collection media, biological sample, viability, extraction, detection, identification

TECHNICAL POINT OF CONTACT: CWMD.SBIR@hq.dhs.gov

SBIR TOPIC NUMBER: DHS201-011

TITLE: Development and Evaluation of Nucleic Acid-Based Assays to Accelerate Biohazard Detection

TECHNOLOGY AREAS: Integrated Detection and Identification, Situational Awareness, Faster Decision Making Capabilities, Sensor Platform for Biohazard Detection

OBJECTIVE: Develop field deployable nucleic acid-based assays to detect and identify biological pathogens in an uncontrolled environment.

DESCRIPTION: Nucleic acid-based diagnostics, also called nucleic acid test (NAT) or nucleic acid amplification test (NAAT), is a technique used detect the presence of a nucleic acid, virus, or bacteria pathogen either by directly detecting the presence of DNA or RNA nucleic acids in the host or by first amplifying the pathogen DNA or RNA[1]. The Department of Homeland Security (DHS) Countering Weapons of Mass Destruction (CWMD) Directorate is pursuing the development of reliable, field deployable, cost-effective, highly-validated, and sustainable polymerase chain reaction (PCR) assays with positive controls. The associated information (e.g. design, limitations) of these assays must be strictly controlled due to its potential use in the national security application. CWMD seeks to fund commercial research that yields novel methods for rapidly identifying, within 30-45 minutes, nucleic acid sequences associated with biological pathogens. The ability to sequence small quantities of starting materials is of particular interest.

PHASE I: Demonstrate a proof of concept of field deployable nucleic acid-based biological detection and identification assays. Phase I deliverables include monthly progress reports and a final Phase I report. Project review meetings will be held at the initiation, mid-point and completion of the Phase I effort.

PHASE II: This phase will expand upon Phase I, conducting the actual research and development to integrate field deployable nucleic acid-based biological detection and identification assays into current and emerging CWMD biodetection efforts. This phase will demonstrate and deliver a reliable, field deployable, cost-effective, highly-validated, and sustainable PCR assays with positive controls.

Phase II deliverables include monthly progress reports and annual technical reports. At least one prototype will be delivered to CWMD (or its partners, as directed) at the end of Phase II. Project review meetings will be held throughout the project period as needed to include but not limited to the initiation, mid-point and completion of the Phase II effort.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: Phase III activities would include a successful commercialization strategy for supporting the integration of or novel technologies into the current or emerging CWMD biological detection and identification efforts. This phase will also include the ability to mass produce this technology.

REFERENCES:

1. What is Nucleic Acid-based Diagnostics? (http://globalhealthprimer.emory.edu/targets-technologies/nucleic-acid-based-diagnostics.html)

KEY WORDS: assay, polymerase chain reaction, nucleic acid, sequence, diagnostic

TECHNICAL POINT OF CONTACT: CWMD.SBIR@hq.dhs.gov