FY 17 Small Business Innovation Research (SBIR) RESEARCH TOPICS

S&T Directorate Topics

The following are the topics for the FY17.1 S&T Directorate's SBIR Program:

H-SB017.1-001 - Enhanced Agent Situational Awareness in Dismounted, Low Light/Adverse Conditions
H-SB017.1-002 - Video Analytics for Homeland Security Missions
H-SB017.1-003 - Do Not Spoof Services for Modern Telephony
H-SB017.1-004 - Identity Verification & Validation for Mobile Networks Authentication Enhancement
H-SB016.1-005 - Blockchain Applications for Homeland Security Missions
H-SB017.1-006 - Wearable Chemical Sensor Badge
H-SB017.1-007 - Over-the-air Authentication Technology for Messaging via Emergency Alerts

Specific details for each topic are included in this **Appendix A**.

DNDO Topics

The following are the topics for the FY17.1 DNDO SBIR Program:

H-SB017.1-008 - Accelerated Crystal-Size Scale-Up Development of Thallium-based, High Efficiency, Dual or Tri-Mode Elpasolite Scintillator
H-SB017.1-009 - Unattended Radiation Detection System

Specific details for each topic are included in **Appendix A**.

APPENDIX A – RESEARCH TOPIC DESCRIPTIONS

SBIR TOPIC NUMBER: H-SB017.1-001

TITLE: Enhanced Agent Situational Awareness in Dismounted, Low Light/Adverse Conditions

TECHNOLOGY AREA: Border Security and Surveillance

OBJECTIVE: Develop and demonstrate an innovative, agent-portable device to augment agent ability while walking, running, hiking, on ATV/motorcycles, horses, boats, and mountain bikes, to automatically detect, identify, classify, and track an item of interest in challenging border terrains comprised of heavy vegetation, mountains, hills, canyons and dry creeks, rivers, streams found in desert, shorelines, open prairies, semi-arid, and heavily forested environments that have been enshrouded with fog, blowing salt/dust, extreme haze or other naturally occurring or adversary-produced vision obscurations such as smoke and irritants encountered in twenty-four (24) hour operations

DESCRIPTION: Border Patrol Agents often encounter situations where a single individual, or groups (2 to 20+) of individuals, illegally cross the International border (fence, river, lake, and littoral) and attempt to evade apprehension into the United States territory. These individuals and groups often synchronize their border incursions during all shifts, to coincide with seasonal adverse weather (wind, dust, fog, rain, snow, sleet, and hail) and man-made (causing dust/muddy) events to also include smoke, dust, or other vision obscuring situations. These individuals also attempt to avoid detection by hiding or blending in among naturally occurring trees, shrubs, hills, draws, man-made structures. In many instances there are no access roads to enable pursuit by a patrol car or 4-wheel drive vehicle, and in most cases the agent pursues on foot.

During these pursuits, an agent must focus on immediate elements of their surroundings: avoiding tripping, falling, and colliding with hazards while simultaneously reading and interpreting ‘sign’ left by fleeing adversaries (footprints, disturbed soil, broken branches, human litter, etc.). The agent has to maintain eye and ear contact with these individuals, and exhibit a self-protection posture to detect and/or avoid a trap/ambush. All of this activity is repeated by an agent over and over while exerting tremendous physical effort compounded by extreme temperatures (125 ° F to -40° F) and adverse weather.

The end-state of this SBIR is to demonstrate a prototype of a man-portable, ruggedized product or device that enables the agent to detect, identify, classify, track, and apprehend individuals attempting to avoid capture while taking advantage of adverse weather and other vision or aural obscurations as described above. The device should provide agents the ability to determine if

individuals are in possession of weapons (side arms, long arms, clubs, sticks, rocks, digging implements, etc.) and/or bundles. It should also allow the agent to determine if the item of interest is human or other (described in table below). The device or product should contain a high degree of automation so that agents will not have to continually focus, tune or otherwise adjust the device to rapidly changing conditions (distance focus, EO to IR/Thermal change). The device should be small enough to be carried and utilized by the average size border agent. It shall preferably not occupy an agents hands and integrate into the existing field kit consisting of a uniform, patrol belt, sidearm, and headgear. It should be secure enough to stay in place during strenuous and exaggerated body movements, and not be affected by sweat, brushing of low hanging tree limbs, sage brush or brief encounters against terrain while walking, running, hiking, on ATV/motorcycles, horses, boats, and mountain bikes. The device should incorporate image stability when in use. Use of this device or product should not cause an elevated user core temperature since many border environments are known to be very hot and dry and the weight of the unit should not exceed twelve (12) ounces. The device should be rugged enough to be impervious to moisture and still operate if dropped. The device should provide GPS coordinates for Individuals of Interest (IoIs) being observed and tracked by the user. The device should have a directional display (North, South, East, West, NE, etc.) for agent reference. The controls knobs or surfaces shall be of an easy to touch or feel controls (rubberized, textured surface knobs, etc.) and instructions and training for use shall be intuitive to the average agent. Battery life should span at least 8 hours (threshold) and 10 hours (objective) of constant use in the most demanding situation and the fuel cell should be rechargeable thru common means: car charger, USB port, solar, etc. The fuel cell and charging system must not be of a proprietary design and should use readily available, over the counter rechargeable batteries, and charging cable with current USB and device cable end.

Additional Desired SBIR Requirements Table:

Requirement	Threshold	Objective
Cost	**≤ $20,000**	**≤ $25,000**
Weight of solution	**≤ 2 pounds**	**≤ 12 ounces**
Electro-Optical/Infra-Red/Thermal imaging	**24 hours**	**24 hours**
Detection of an individual person or group (2-20) from agent/user to:	**1 mile**	**≥ 5 miles**
Identify between person or non-person (animal or conveyance) from agent/user to:	**1 mile**	**≥ 5 miles**
Classify, or distinguish between agent and adversary (armed/unarmed/carry bundles) from agent/user to:	**1 mile**	**≥ 5 miles**

Tracking of IoIs (individual walking, on a horse, on an ATV, on a boat/raft, or a vehicle) from agent/user out to:	**1 mile**	**≥ 5 miles**
Power source for device	**Rechargeable COTS batteries**	**Rechargeable COTS battery**
Power charge sustainment	**≥ 8 hours**	**≥ 10 hours**
Security	**No function if lost or stolen**	**No function if lost or stolen**
Ruggedization-device should be able to withstand being dropped from ___ feet while being used.	**10 feet AGL**	**20 feet AGL**

PHASE I: Provide a proof of concept viability with an illustrated hardware design that depicts the necessary requirements and technical solution to include, at minimum a block diagram of system, and any required on-board computing software mock-up of the main and ancillary hardware units. Briefly describe a general usage CONOP which will be used as a starting point for proposed Phase II testing and demonstration of two operational prototypes.

PHASE II: Build a functional prototype and conduct a feasibility study to identify concept impact to the stated mission and establish the necessary partnerships with industry to define integration methodologies to include hardware and software designs and required network interactions (if applicable). Test the prototype in border area operational surroundings.

PHASE III: The proposed technology refined into an appropriate design for operational use by border agents to respond to border incursions on foot, horseback or ATV. Continue Border Patrol field assessments leading to decisions for potential commercialization of the product or device.

REFERENCES:

1) US Customs and Border Protection, *Vision & Strategy 2020* (available for download at https://www.cbp.gov/document/publications/vision-and-strategy-2020)
2) US Customs and Border Protection, 2012 – 2016 *Border Patrol Strategic Plan*, (https://www.cbp.gov/sites/default/files/documents/bp_strategic_plan.pdf)

KEYWORDS: Augmented visual, augmented aural, border protection, border patrol, force protection, protection, self-tracking, automatic tracking, border security, situational awareness,

Homeland Security, rapid response, information, interoperability, emerging technologies, search, rescue.

TECHNICAL POINT OF CONTACT: MK Tribbie mk.tribbie@hq.dhs.gov

SBIR TOPIC NUMBER: H-SB017.1-002

TITLE: Video Analytics for Homeland Security Missions

TECHNOLOGY AREAS: Surveillance, Video Analytics, Classification, Identity

OBJECTIVE: Develop a software video and image analytic tool that can be placed at remote sites which enables the application of user-defined parameters, attributes or behavior patterns to identify activities of interest, while minimizing false alarms from both infrared and electro optical sensor data.

DESCRIPTION: DHS is seeking innovative solutions for using video analytics to identify activities of interest in near real time within still images or streaming video feeds, or in archived video data for forensic analysis. The analytic tool will allow users to apply filters to identify objects, events, attributes or patterns of behavior in a scene; activities meeting user applied criteria will be used to alert operators and / or initiate recording of video.

Homeland Security missions rely heavily upon video surveillance for detection and attribution of nefarious activities using real time monitoring or through forensic analysis of recorded video. Operators become overwhelmed when monitoring large numbers of video feeds and become increasingly ineffective over long shifts. In a similar fashion, analysts reviewing hours or days of recorded video to find a specific event become increasingly ineffective and prone to human error.

DHS desires video analytic solutions which enable users to select or define parameters that may be programmed to automatically identify objects, events, attributes or patterns of behavior; when identified by the analytic tool, near real time alerts will be provided to an operator and / or initiate recording for forensic analysis. Particularly in complex outdoor environments, this requires the application of multiple parameters to lower the false and nuisance alarm rates to acceptable levels. Examples of parameters which users should be able to select or define include:

- Direction of movement
- Velocity of movement
- Acceleration or deceleration of a person or other item of interest above “normal”
- Human vs non-human, vehicles, air platforms, vessels
- Polygon within a scene where activity should be excluded or included
- Size and / or shape of an object
- Color of an object
- When 2 or more objects (human or non-human) meet or approach within a specified distance of one another

- When an object (human or non-human) is stationary within a scene for a specified period of time
- Redaction of a user-identified object or region within a scene
- Facial detection (not identification)

Once parameters are programmed, the video analytic tool should operate autonomously with live video feeds or snapshot images from cameras currently used for border surveillance and Law Enforcement investigations. This same tool should also be capable of the same functions when used on archived video; only select segments (based on the new forensic tool's sorting function) of video meeting the user-specified parameter(s) would be copied and saved for an analyst to review, thus creating a more manageable set of data for forensic use.

PHASE I: Video analytics have been used in other applications but the uncontrolled environmental conditions experienced for border surveillance and Law Enforcement investigations are more severe, particularly with respect to dynamic lighting conditions, heat scintillation, the effects of wind and windblown clutter and dust, the presence of wildlife, and precipitation. The proposed approach needs to address how these environmental issues will be addressed and mitigated, and the Phase I work shall demonstrate the viability of the proposed approach using sample video and snapshots provided by DHS. The proposed approach will address how with no item of interest present, background imagery that changes due to lighting or weather will be assessed, to prevent false alarms.

PHASE II: The Phase II effort will provide a prototype analytic software toolset which allows integration of existing tools using Application Programming Interface(s) (API). The toolset will have a Graphic User Interface (GUI) allowing users to intuitively select and apply multiple parameters to filter activity(s) contained within the video to identify and alert when specific objects, events, attributes and / or patterns of behavior occur. The software should run on still images, live video feeds as well as archived video. The Phase II effort should include a demonstration of the prototype configuration to be completed using at least two DHS provided video(s) and / or live video feeds to establish metrics for comparison to traditional analytic techniques requiring manual review. Phase II efforts will be focused on imagery and video from a desert environment.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: Refine the prototype GUI and add tools able to be selected and applied by users. Ensure the product is able to run smoothly on standard PC desktop computers or laptops in real time. Conduct an Operational Assessment for user evaluation of the capability in desert and urban operational environments.

REFERENCES:

1) C.Szegedy, A. Toshnov, and D. Erhan, “Deep neural networks for object detection” in Annual Conference on Neural Information Processing Systems, 2013, pp. 2553 – 2561.
2) Andrzej Czyżewski, Grzegorz Szwoch, Piotr Dalka, Piotr Szczuko, Andrzej Ciarkowski, Damian Ellwart, Tomasz Merta, Kuba Łopatka, Łukasz Kulasek and Jędrzej Wolski, “Multi-Stage Video Analysis Framework, Video Surveillance” (2011): Intech, http://www.intechopen.com/books/video-surveillance/multi-stage-video-analysis-framework n. pag.
3) Ng, Ka Ki, and Edward Delp J. "Object Tracking Initialization Using Automatic Moving Object Detection." Visual Information Processing and Communication (2010): n. pag. Print
4) Ka Ki Ng, Edward J. Delp, “Background Subtraction Using A Pixel-Wise Adaptive Learning Rate For Object Tracking Initialization” in Proceedings of the IS&T/SPIE Conference on Visual Information Processing and Communication, volume 7882, San Francisco, California, January 2011.
5) Ka Ki Ng, and Edward J. Delp "Object Tracking Initialization Using Automatic Moving Object Detection." Visual Information Processing and Communication (2010): n. pag. Print.

KEY WORDS: video analytics, video surveillance, video forensics, detection, classification

TECHNICAL POINT OF CONTACT: John Thayer, john.thayer@hq.dhs.gov

SBIR TOPIC NUMBER: H-SB017.1-003

TITLE: Do Not Spoof Services for Modern Telephony

TECHNOLOGY AREAS: Cyber Security, Emergency Response, and Communications

OBJECTIVE: Develop tools that can be deployed in a cyber ecosystem or carrier network to detect and block spoofed phone calls.

DESCRIPTION:

The shift from land-line phones to mobile devices and Voice over IP (VoIP) has enabled new types of call spoofing where an adversary appears to be coming from a number or location. For example, an adversary attempting to defraud taxpayers may appear to be coming from an IRS 800 help number or an adversary attempting to install malware on a government system may appear to be coming from an agencies tech support number. In both cases, the adversary appears to be coming from a trusted number but in fact has no relationship to that trusted number. In a related case, the adversary may spoof the call location. For example, an adversary may falsely report being on a vessel that requires emergency assistance. By providing a false number and false location, the adversary may cause limited resources (such as search and rescue teams) to be deployed in response to a non-existent emergency. In all cases, the adversary's ability to easily spoof a caller's number and location is a substantial challenge that this SBIR effort aims to address.

PHASE I: Phase I proposals should provide an initial proof of concept design document for detecting and blocking spoofed messages. There are three use cases and a proposal could address one or more of the use cases. The first use case is an organization that wants to prevent others from spoofing its phone numbers. One can assume the organization has numbers that are known in advance and should never place outgoing calls. An example is help desk numbers where taxpayers can call the IRS, but these numbers are never used to place outgoing calls to taxpayers. The second case focuses on an organization's ability to block spoofed external calls. An example is an organization that wants to ensure no one can call its employees mobile phones and spoof a number that appears be coming from within the organization. The third use case is to identify calls whose reported location is spoofed. An example would be a call that appears to be coming from offshore when in fact the call is originating from an onshore location. The proof of concept design could consist of software systems, embedded devices, monitoring tools, or combination of each of these elements that address one or more of the use cases. Phase I deliverables will also include monthly reports, a technical demonstration, and final report.

PHASE II: A prototype device or software capable of deployment to address any of the three use cases identified above. The prototype device must be applicable to mobile devices and VoIP systems. The developed prototype will be delivered to DHS for piloting. The component should leverage applicable and operational best practices for the intended environment.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: Refine components from Phase II, and work with an agency or organization to deploy the resulting solution.

REFERENCES:

1) IRS Warns of Pervasive Telephone Scam - https://www.irs.gov/uac/newsroom/irs-warns-of-pervasive-telephone-scam
2) Beware of Voice Phishing or "Vishing" Calls - http://www.ag.state.mn.us/Consumer/Publications/VoicePhishing.asp
3) Coast Guard seeks serial hoaxer whose calls for help cost $500,000 - http://www.foxnews.com/us/2016/07/25/coast-guard-seeks-serial-hoaxer-whose-calls-for-help-cost-500000.html

KEY WORDS: Telephony, VoIP, Spoofing, Do Not Call, Vishing, Attribution, RoboCalls

TECHNICAL POINT OF CONTACT:

Dr. Dan Massey, Daniel.Massey@hq.dhs.gov
Dr. Ann Cox, Ann.Cox@hq.dhs.gov

SBIR TOPIC NUMBER: H-SB017.1-004

TITLE: Identity Verification & Validation for Mobile Networks Authentication Enhancement

TECHNOLOGY AREAS: US Mobile Networks, 5G, DHS Priority Service

OBJECTIVE: Research and develop new methods for mobile network authentication enhancements by leveraging commercially available financial infrastructure to perform mobile user identity verification/validation. This new enhancement(s) shall not impact the standardized authentication procedures/process (e.g. the authentication procedures standardized in 3rd Generation Partnership Project).

DESCRIPTION:

Authentication is essential and has been implemented at different levels including user authentication, device authentication, and application authorization/authentications. In general practice, commercial mobile networks do not perform user verification/validation after the initial user (subscriber)/device activation/registration/authentication processes unless device is lost/stolen. The owner (subscriber) of a device is responsible for any services originated/terminated on this device regardless of who may be using the device at a time. A security enhancement for user identity verification/validation on-demand on top of the standardized authentication implemented in mobile networks is desired, and essential for services such as DHS Priority Services.

PHASE I: (1) Conduct feasibility study for utilizing existing financial network infrastructure to perform secure and reliable user identity verification/validation without modification of the standardized authentication procedures/process in commercial mobile networks; (2) investigate and identify other identity verification/validation on-demand solutions in conjunction with standardized mobile network authentication mechanisms, and generate solution comparison metrics.

PHASE II: (1) Out of phase-I outcomes, identify gaps/requirements on how to link/bridge/implement the user identity verification/validation in conjunction with standardized authentication solution in commercial mobile networks; (2) Develop a solution to allow Priority Service subscriber invoke/revoke priority services from any mobile device without inducing unauthorized service access attempts. (3) Perform system concept approval and demonstration in an agreed lab environment. (4) Reach out to the commercial network service provider(s) to propose and perform pilot demonstration(s). Suggest and recommend transition from the pilot solution to the commercial use in support of DHS Priority Service and/or any other potential services.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: Plan and execute transition from the pilot solution into commercial use to support DHS Priority Service and/or any other potential services.

REFERENCES:

1) Public Safety Entity Control and Monitoring Requirements for the Nationwide Public Safety Broadband Network, Final Report October 2015
2) The State Identity Credential and Access Management Guidance and Roadmap (SICAM), NASCIO, 2012
3) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Identity management and 3GPP security interworking; Identity management and Generic Authentication Architecture (GAA) interworking (Release 12)
4) NIST Special Publication 800-63-2, Electronic Authentication Guideline
5) Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance

KEY WORDS: Identity Management, Credentialing, Public Safety, FirstNet, Cellular, LTE, 4G, 5G, NPSBN.

TECHNICAL POINT OF CONTACT:

DHS S&T HSARPA CSD
Vincent Sritapan, vincent.sritapan@hq.dhs.gov
DHS NPPD OEC
Gabriel A. Martinez, gabriel.a.martinez@hq.dhs.gov.

SBIR TOPIC NUMBER: H-SB016.1-005

TITLE: Blockchain Applications for Homeland Security Missions

TECHNOLOGY AREAS: Identity, encryption, authentication, cyber security, internet of things, and data analytics

OBJECTIVE: Design and prototype an ecosystem that applies blockchain technology to significantly improve DHS analytics, missions, and operations. Proposed solutions should be focused on new applications of blockchain technology and not focused purely on the analysis and characterization of Bitcoin or other cryptocurrency transactions.

DESCRIPTION: Blockchain technologies potentially offer a very flexible, low cost, and secure means of implementing data analytics architectures. In the virtual currency world, blockchains are distributed ledgers that keep track of all transactions authenticated by thousands of independent users' machines. This process, called mining, inherently makes the ledger extremely difficult and expensive to hack. The use of machines to authenticate transactions makes authentication more cost effective. Virtual currencies like bitcoin have a governing body that manages and updates the algorithms for transactions and rules for user participation. Numerous entities – banks, technology companies, etc. – are exploring blockchain applications for the future. DHS can benefit from solutions that offer this level of flexibility, security, accountability and cost. To maximize cost savings and effectiveness, blockchain applications should operate in a limited trust environment, which emphasizes need for decentralized rules, decentralized transactions, traceability, and defined ownership.

Use cases may include, but are not limited to crypto-certified transactions involving users and devices for the internet-of-things applications (IoT) such as encrypted data transactions and analytics for first responders; information sharing and analysis between state, local, and federal law enforcement; and third parties' involvement, perhaps in applications that improve security and experiences for the traveling public, or that improve bio-threat awareness. Proposers may define relevant use cases and architectural concepts where there is a significant value proposition for the homeland security enterprise.

Proposed solutions can involve open environment blockchain applications such as cryptocurrencies, where anyone can participate, and closed-permissions based environments. Regardless of the architecture, privacy is an important DHS priority for use cases that might involve any personally identifiable information (e.g., biographical, biometric). National computer and network security policies and standards are also important considerations. For scalability, solutions must also consider speed of analysis and any transaction validation capabilities.

PHASE I: Design an application ecosystem, analytics methodology and approach for applying blockchain technology to significantly improve or enable homeland security applications and use cases. Produce an architecture that leverages existing or creates algorithms and computational techniques; show how components and services function in the ecosystem; and develop an approach for building and maintaining this ecosystem. Demonstrate or discuss implementation feasibility with respect to: concept of operations, governance, algorithms, costs, and security. Identify risks to privacy, security, and technology and develop risk mitigation strategies.

PHASE II: Prototype the ecosystem(s), including purchasing or making equipment needed. Implement and refine system modules and algorithms. Demonstrate prototype(s) and algorithms in a laboratory environment with data that reflects proposed homeland security applications and use cases. Demonstrate general core capabilities by developing and demonstrating multiple but disparate applications from the same core product capabilities. Refine the architecture and technical approach based on feedback from the government and marketplace as appropriate for selected applications. Demonstrate improvements after refinements and feedback. Initiate transition/commercialization options that leverage the strengths of demonstrated results, market demand and homeland security value propositions.

PHASE III: Deploy the first version products for operational testing, verification and validation for specific homeland security use cases. Fully implement transition options for use by DHS Components, the homeland security enterprise or related dual use commercial opportunities.

REFERENCES:

1) https://www.cryptocoinsnews.com/mit-digital-currency-initiative-leader-government-officials-lets-get-open-data-2-0-moving/
2) http://www.coindesk.com/block-chain-aid-fight-free-speech/
3) http://www.coindesk.com/blockchain-rise-networked-trust/
4) http://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things/
5) http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=XB&htmlfid=GBE03620USEN
6) http://www.coindesk.com/four-genuine-blockchain-use-cases/
7) http://www.coindesk.com/8-banking-giants-bitcoin-blockchain/
8) http://www.technologyreview.com/news/539171/why-nasdaq-is-betting-on-bitcoins-blockchain/

KEY WORDS: Identity, encryption, authentication, cyber security, internet of things, and data analytics

TECHNICAL POINT OF CONTACT: Stephen Dennis, Stephen.Dennis@hq.dhs.gov;
Alex Phounsavath, Alexandria.Phounsavath@hq.dhs.gov

SBIR TOPIC NUMBER: H-SB017.1-006

TITLE: Wearable Chemical Sensor Badge

TECHNOLOGY AREAS: Emergency preparedness and response, smart devices, wearables, warning and notification, chemical defense

OBJECTIVE: Develop a prototype wearable chemical sensor badge that responds to multiple Toxic Industrial Chemicals (TICs). This wearable badge must be able to respond to its immediate surroundings with naturally diffused air or a sample pump of appropriate size and sound profile. This effort must thoroughly study the cross sensitivity between different target chemicals and the effect of common interferents and environmental conditions in order to minimize false alarms.

DESCRIPTION:

The wearable chemical sensor dimensions should not exceed 2x2 inches with a maximum of 0.5 inches in thickness ("badge"). Ultimately, the approach should be amenable to being configured as a button as part of a first responder uniform. The badge should have more than one type of alarm indicator (such as visible and audible alerts, visible and vibration alerts, etc). The response time of the sensor should have an objective of one second or a threshold of 30 seconds. The sensor badge should have a shelf like of at least twelve month (storage in package) and weigh less than 100g including the batteries. The cost of the badge should be affordable (objective: $30; threshold: $50). If appropriate, the vendor should propose disposable sensing elements at less than $5 per element with a reusable badge casing. The developed prototype badge should respond to at least four high priority TICs down to the permissible exposure limits (PEL) with negligible false alarm rate. Suggested TICs are provided in Table 1 (priority order).

Table 1. TIC Targets in Priority Order

Toxic Industrial Chemicals
Chlorine (Cl_2)
Carbon Monoxide
Hydrogen Sulfide
Carbon Dioxide
Nitrogen Dioxide
Methane
Ammonia
Hydrogen Cyanide
Phosphine
Methyl Bromide

PHASE I: Demonstrate the feasibility of the proposed sensing approach by providing performance data with one TIC from Table 1. The performance data must include results of the TIC in the presence of interferents (e.g., smoke) and varying environmental conditions (-20 to +50 °C) and humidity range (10-90% RH). The Phase I final report must include a Computer-Aided Design of the sensor and information on the following: (1) anticipated sensitivity and selectivity; (2) anticipated response time for the four TIC targets; (3) anticipated size and weight of final product; (4) power requirements and length of operation time before recharge; (5) training requirements; and (6) anticipated maintenance and operation costs. The report must also include anticipated risks and mitigation strategies and ideas for commercialization.

PHASE II: Fabricate at least six prototype badges and demonstrate their operation in a simulated environment in the lab with selected TICs and interferents. The sensors must alarm at high/low conditions where low is PEL concentrations and high is Short Term Exposure Limit (STEL) or Time Weighted Average (TWA) concentrations (Table 2).

Table 2. TIC Detection Limits

	OSHA PEL (ppm)	NIOSH REL (ppm)
Ammonia	50	25 (TWA) 35 (STEL)
Carbon Dioxide	5000	5,000 (TWA) 30,000 (STEL)
Carbon Monoxide	50	35 (TWA) 200 (Ceiling)
Chlorine (Cl_2)	1	0.5 (TWA) 1 (STEL)
Hydrogen Cyanide	10	4.7 (STEL)
Hydrogen Sulfide	20 (ceiling)	10 (Ceiling)
Methane	There are no specific exposure limits for Methane. Methane is a simple axphyxiant. Oxygen levels should be maintained above 19.5%.	
Nitrogen Dioxide	5 (ceiling)	1 (STEL)
Phosphine	0.3	1 (STEL)

Methyl Bromide	20	19 (TWA)

PHASE III: The proposed wearable chemical sensor badge would find applications in government, public and private sector as dual-use technology. The contractor shall explore the suitable engineering tests for a field evaluation of the developed prototype and identify suitable pathways for commercialization within these sectors.

REFERENCES:

1) Regulations and You: TICs, TIMs and Terrorism. Bennett, M. Today's Chemist at Work. American Chemical Society. Apr. 2003, Page 21-25.
2) Guide for the Selection of Chemical Agent and Toxic Industrial Material Detection Equipment for Emergency First Responders. U.S. Department of Homeland Security. Guide 100-06 3rd Edn. Jan. 2007.

3) Testing and Evaluation of Handheld Toxic Industrial Chemical Detectors. Technology Evaluation Report by EPA. Aug. 2012 EPA 600/R-12/560.
4) Janata, Jiri. *Principles of Chemical Sensors*, Plenum Press, New York, (1989).

KEY WORDS: Chemical Sensor, wearable sensor, smart devices,

TECHNICAL POINT OF CONTACT: Angela M. Ervin, Ph.D., angela.ervin@hq.dhs.gov

SBIR TOPIC NUMBER: H-SB017.1-007

TITLE: Over-the-air Authentication Technology for Messaging via Emergency Alerts

TECHNOLOGY AREAS: Alerts, Warnings, and Notifications (AWN); Wireless Emergency Alerts (WEA); Cybersecurity; Information Sharing; Interoperable Communications

OBJECTIVE: Develop and demonstrate a mechanism that authenticates messages sent via Wireless Emergency Alerts, notifies the recipient(s) of the authentication status of such messages, and proves resilient to spoofing of such messages.

DESCRIPTION: Wireless Emergency Alerts (WEA) use commercial cellular networks to disseminate emergency messages to cell phones in a specific geographical area. WEA notifications include child abductions (e.g., AMBER Alerts); imminent threat messages, such as severe weather, shelter-in-place, and "wanted alerts" – such as the one recently issued on September 19, 2016 following the bombings in New Jersey and New York City; and Presidential messages. WEA messages are limited to 90 characters currently and are sent securely by government alerting authorities to commercial cellular network operators using the common alerting protocol (CAP). These operators use the Cell Broadcast to send a WEA message to cell phones.

This solicitation seeks a novel approach to authenticate WEA messages received via Cell Broadcast. Such an approach will prevent potentially unauthorized messages from being mistaken for authorized WEA messages. The solution will provide a notification to the recipient of the authentication status of such messages. Additionally, the solution must be resilient to any type of spoofing of WEA messages (e.g., false messages that may originate from sources other than approved government alerting authorities). The solution shall demonstrate a strong understanding of the WEA architecture, the common alerting protocol, cellular broadcast technologies, and major cell phone operating systems. Solutions should focus on technologies that do not require changes to the underlying cellular standards but may include imminent updates to those standards. Additionally, solutions should limit dependencies on specific cell phone operating systems.

PHASE I: The vendor shall prepare an engineering concept report that (a) details a solution that meets the requirements given in the description section of this solicitation, (b) clearly describes the threat profiles that the solution will mitigate, and (c) identifies the limitations of the solution.

Phase I deliverables shall include: engineering concept report as previously described; a short monthly technical and program report that provides task descriptions, percentage completed, targeted completion date, risks, etc.; and a monthly status call to discuss the monthly report.

PHASE II: The vendor shall develop and demonstrate the solution to authenticate messages sent via Wireless Emergency Alerts. DHS S&T will work with the vendor to coordinate a meaningful demonstration environment. The demonstration not only will include the handling of genuine WEA messages but also false WEA messages according to the threat profiles described in the engineering concept report. The demonstration shall be performed on multiple cell phones types as defined in the vendor's proposal.

Phase II deliverables shall include: a kick-off meeting; a short monthly technical and program report that provides task descriptions, percentage completed, targeted completion date, risks, etc.; a monthly status call to discuss the monthly report; an engineering reference design document for the solution; a working prototype that authenticates messages sent via Wireless Emergency Alerts, notifies the recipient(s) of the authentication status of such messages, and proves resilient to spoofing of such messages; and a demonstration that will produce a test and evaluation matrix.

Finally, vendors shall assist DHS S&T Communications, Outreach, and Responder Education (CORE) personnel develop and review communications materials related to the solution.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: A successful solution may produce intellectual property – and/or one or more specific implementations – for message authentication (of WEA messages over cell broadcast). Other types of message services using cell broadcast may also benefit from such an authentication mechanism. Thus, the radio access networks (including all cellular handsets) of participating cellular service providers in the United States become the potential addressable market for such a successful solution.

REFERENCES:

1) Frequently Asked Questions: Wireless Emergency Alerts (12/21/2015), https://www.fema.gov/frequently-asked-questions-wireless-emergency-alerts
2) Common Alerting Protocol (12/11/2015), (https://www.fema.gov/common-alerting-protocol
3) Integrated Public Alert & Warning System (09/16/2016), https://www.fema.gov/integrated-public-alert-warning-system
4) Feasibility Study for WEA Cell Broadcast Geo-Targeting (12/02/2015), https://access.atis.org/apps/group_public/download.php/25924/ATIS-0700027-FeasibilityStudy.pdf
5) Cell Broadcast (retrieved 09/29/2016), http://www.telecomabc.com/c/cb.html

KEY WORDS: Wireless Emergency Alerts (WEA); Cybersecurity; Alerts and Warnings; Cell Broadcast

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

SBIR TOPIC NUMBER: H-SB017.1-008

TITLE: Accelerated Crystal-Size Scale-Up Development of Thallium-based, High Efficiency, Dual or Tri-Mode Elpasolite Scintillator

TECHNOLOGY AREAS: Radiation detection, scintillators, Elpasolites, CLYC, technology development

OBJECTIVE: Develop multi-mode gamma/neutron detector materials with simultaneous high energy resolution and higher efficiency, as well as good particle discrimination, and especially scale up these crystal materials to sizes of 3" diameter x 3" long right cylinders or larger. Such materials are key to DHS/DNDO efforts in advancing new detector technologies for the Global Nuclear Detection Architecture (GNDA).

DESCRIPTION: Gamma-ray and neutron detection plays an important role in the identification of radiological materials and threats. Gamma-ray detectors mainly utilize crystalline scintillation materials, which are required to have good energy resolution and high detection efficiency. Dual or tri-mode crystal materials, such as Ce-doped CLYC (Cs2LiYCl6:Ce) have been developed and commercialized, and their sizes have been steadily increasing. The 6Li in CLYC is sensitive to thermal neutrons, whereas the Cl is sensitive to fast neutrons. By appropriately choosing whether the Lithium (Li) is enriched 6Li or enriched 7Li, one can taylor the neutron sensitivity to either predominantly thermal neutrons or fast only neutrons. In addition, CLYC offers good energy resolution for gammas in the low 4% range at 662 keV. The unique properties of CLYC has resulted in great interest from the rad/nuc community. However, comparison testing has shown that its efficiency is not as good as traditional COTS materials such as NaI or CsI. Fortunately, initial results from a variant of CLYC, namely TLYC (Tl2LiYCl6:Ce), wherein the Cs has been replaced with Thallium, has demonstrated potentially similar performance to CLYC but with enhanced efficiency of gamma detection. The enhanced efficiency is due to the facts that TLYC is 33% more dense, and has a higher effective Z of 71 versus 46 for CLYC. The purpose of this topic area is to leverage the learning curve from CLYC development and apply it to an accelerated scale up development effort for TLYC or TLYB (Br replacing Cl).

PHASE I: The goal of this phase is to first demonstrate the capability of producing small high performance crystals of TLYC, and secondly to show initial progress of successfully scaling up the crystal sizes without sacrificing performance. Good performance equates to better than 4.3% energy resolution for 1 cm3 or larger crystals, with FOM of 2.0 or better wherein FOM is defined as separation of gamma and neutron distribution divided by sum of FWHM of the neutron and gamma distributions in a PSD (Pulse Shaped Discrimination) plot of the vendors choosing. The progress toward scale-up needs to be demonstrated by the end of Phase I by achieving at least two crystals of 1" dia x 1" long

sized with comparable performance to that of the smaller crystals.

The proposal must provide a phased technical approach leading to a feasibility demonstration at the end of Phase I addressing all critical technical issues and risks and mitigation strategies.

PHASE II: The goal of Year 1 of Phase II will be to produce 2" diameter x 2" long right cylinders of Tl-based elpasolites with comparable performance to the 1" versions. The goal of Year 2 of Phase II will be to produce 3" diameter x 3" long right cylinders of the Tl-based elpasolite with comparable performance to the 1" versions.

Vendor may enter directly into Phase II if they have satisfied the goals of Phase I at the beginning of the contract.

PHASE III - COMMERCIAL OR GOVERNMENT APPLICATIONS:

DNDO expects this technology to be utilized in targeting illicit trafficking and unauthorized use of nuclear and radiological material, and to help protect against both nuclear and radiological terrorism. Specifically, it would be integrated into passive and active detection equipment used for assessing situations in which radiation is being emitted and/or radioactive materials are expected to exist. Further uses include basic science research (nuclear, radiochemistry), astronomical gamma ray imaging and nuclear medicine (SPECT, PET) and x-ray imaging.

REFERENCES:

R. Hawrami; E. Ariesanti; L. Soundara-Pandian; J. Glodo; K. S. Shah, "Tl2 LiYCl6 :Ce : A New Elpasolite Scintillator," in IEEE Transactions on Nuclear Science , vol. PP, no.99, pp.1-1, doi: 10.1109/TNS.2016.2627523

J.Glodo, R.Hawrami, K. Shah, Development of Cs2LiYCl6 scintillator, Journal of Crystal Growth, Volume 379, 15 September 2013, Pages 73-78

KEY WORDS: Radiation detector, scintillator, spectroscopy

TECHNICAL POINT OF CONTACT: DNDOSBIR@hq.dhs.gov

SBIR TOPIC NUMBER: H-SB017.1-009

TITLE: Unattended Radiation Detection System

TECHNOLOGY AREAS: Radiation detection, unattended sensors, real-time detection, data fusion

OBJECTIVE: Research will support the development of an unattended radiation detection system. The product should be capable of radiation detection and analysis, capture relevant contextual information (e.g., video or pictures) from the surrounding environment at times of detection, and integrate into communications relevant to end-users for timely transmission of collected information. The system should have low-energy requirements to facilitate long periods without direct operator interface.

DESCRIPTION: A need has been recognized for radiation detection systems to be located in remote and urban environments with the ability to function fully without physical intervention from an operator. These unattended radiation detection systems should apply real-time spectral detection methods from radiation detectors and combine information from various auxiliary sensors to include, but not limited to video and still cameras. The sensor data associated with these systems can easily saturate the communication bandwidth available as well as the drain the power required to transmit the unprocessed data to a server. Thus, a new system is required to conduct real-time monitoring and analysis at low power levels, and acquire, synchronize, analyze, compress, and communicate data from the multiple sensor components only during times of threat detection. Since communication infrastructure can vary by end-users and regions, the unattended system should be able to integrate into a wide variety of communications networks. Optimized performance benefits include resourceful use of power management, reduced data storage via compression/filtering, reliable two-way communication, and ability to execute advanced algorithms from spectral and video systems.

The resulting system is envisioned to be used as an unattended and rapidly mobilized detection systems for deployment in an outdoor environment of durations exceeding 24 hours with optimized communication protocols that transmit radiation and ancillary sensor (e.g. video) information related to a spectral alarm or as requested remotely.

It is expected that approaches that are tightly configured for a specific use case may not be well-suited for another. However, approaches that are flexible across multiple operating environments are desirable. Approaches that incorporate commercial off-the-shelf (COTS) and scalable, open-source software approaches are also preferred.

PHASE I: Phase I will develop and evaluate a number of technological designs of data acquisition, computational analysis, and communication that may benefit a selected end-user environment. Phase I efforts should directly address that ability to apply the hardware design approach to run the computational applications related to the spectral sensors, auxiliary sensors, communication protocols/controls, data management/compression, and auxiliary sensor. The approach shall include a quantitative analysis of the size, weight, and power requirements and limitations associated with the proposed design. The proposed approach shall provide an estimate of the computational and communication burden and its compatibility with bandwidths available from COTS Bluetooth, Wi-Fi, cellular, and other protocols for remote applications such as satellite.

Phase I shall also look at the quantitative impact of compression, encryption, error-checking, information lag, and stability regarding the data communication to a systems outside the sensor systems such as a server or smartphone.

PHASE II: Phase II activities include the design iterations or spirals associated with selected components and shall culminate in the assessment of the system in a setting comparable to one or more end-user's environment. During Phase II, end-user assessment may provide feedback during the spiral assessment on the operational design and provide documented guidance about modifying (i.e. system must operate only in encrypted WiFi or should include additional environmental sensors).

Phase II should look to develop and demonstrate the interface of the hardware computation with COTS sensors to include the radiation detectors and demonstrate the data outside the system. During Phase II, the offeror will work with the government team to specify the threshold and objective requirements that may be tested in Phase III.

Upon request, the government shall provide specific requirements of a government reference system.

PHASE III - COMMERCIAL OR GOVERNMENT APPLICATIONS: Phase III shall entail the selection of specific application and system requirements associated with the intended end-users. Selection of multiple end-uses may be concurrently assessed in Phase III to include but not limited to existing government systems, COTS systems, or mature prototypes slated for government characterization.

REFERENCES:

Brennan, Sean M., et al. "Radiation detection with distributed sensor networks." *Computer* 37.8 (2004): 57-59.

Arlt, R., and D. E. Rundquist. "Room temperature semiconductor detectors for safeguards measurements." *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment* 380.1 (1996): 455-461.

KEY WORDS: Radiation Detection, Networks, Inertial Measurement Unit, Global Positioning System, Application Programming Interface

TECHNICAL POINT OF CONTACT: DNDOSBIR@hq.dhs.gov