APPENDIX A – RESEARCH TOPIC DESCRIPTIONS

SBIR TOPIC NUMBER: H-SB016.1-001

TITLE: Security Systems Video/Audio Interoperability Device

TECHNOLOGY AREAS: video/audio transmission, video/audio interoperability, security systems, surveillance cameras, security cameras, CCTV, incident command, situational awareness

OBJECTIVE: Develop a prototype video/audio interoperability device that enables authorized users to access video security systems and rebroadcast the signals with the ease of a "plug and play" solution.

DESCRIPTION: First Responders, such as law enforcement and incident command managers, rely heavily on video and audio technology to increase their situational awareness while onsite at an incident, monitoring an incident from afar, or conducting day-to-day response. Security and emergency response operations are often provided for special events, such as National Security Special Events (NSSE, which is defined as an event of national or international significance deemed by DHS to be a potential target for terrorism or other criminal activity) and for various contingency operations with situational awareness often gathered through the provision of video and audio transmissions that are both digital and analog. There is a need for a device that enables plug and play capture of video and audio from existing surveillance systems. Phase I will design a self-contained concept that will capture video and audio from security systems commonly implemented by both public and private entities. Phase II will use the research from Phase I to develop and build the prototype device, and conduct field testing.

PHASE I: The objective of Phase I is to design a self-contained concept that will capture video and audio from closed-circuit and networked security systems commonly implemented by both public and private entities. The concept will address how to access the video and audio feed with the approval of the owners, and rebroadcast it to first responders for improved situational awareness and providing participant safety.

The concept will enable plug and play access, through hard-wired or wireless capability, to the widest array of existing public and/or private video security systems for use during an emergency or response operation. To optimize the ability for authorized DHS components to readily access on-the-scene information, the concept will consider characteristics of typical video and audio security systems installed in buildings or used to monitor large outdoor areas (such as closed-circuit television (CCTV) cameras, networked camera systems, their types of inputs and outputs, encryption systems, and wireless of transmissions).

Deliverables will include a detailed concept design of a self-contained, portable interoperability device which enables the capture and retransmission of video and audio signals. The documentation will identify significant types of video surveillance systems (with estimated percentage of users and complexity of each system type), a proposed methodology for accessing these systems, any partial or quick-win solutions for rapid implementation, and a detailed technical description of the proposed portable device and how it could be used. An additional

deliverable will outline a plan to prevent unauthorized parties to acquire and improperly use the device.

PHASE II: Based on Phase I results, construct and demonstrate the operation of a prototype video interoperability device which enables authorized users to quickly access public and (with appropriate permissions) private systems, for the purpose of providing security and situational awareness.

Deliverables will include a functioning working prototype, a test plan, conduct of a laboratory or field test, and user instructions for operation. In addition, a plan to prevent unauthorized parties to acquire and improperly use the device will address how to transition the final prototype to a product and make it available in the marketplace to authorized users.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: The government application of this technology will be for emergency management oversight at incident command centers and to provide situation awareness support at special security events. These applications may include security, fire, emergency medical services, and emergency management.

REFERENCES:

"Closed-Circuit Television." Wikipedia; The Free Encyclopedia, https://en.wikipedia.org/wiki/Closed-circuit_television

Security Cameras/ Security Systems Fact Sheet: Transit Overview, https://www.pcb.its.dot.gov/factsheets/security/sec_overview.aspx#page=tech

Stowell, Holly. (June 15, 2015). *Surveillance for Security and Beyond*. Retrieved from https://sm.asisonline.org/Pages/Surveillance-for-Security-and-Beyond.aspx

Private Sector Camera Initiative, Chicago Office of Emergency Management and Communications. Retrieved from http://www.cityofchicago.org/content/dam/city/depts/oemc/supp_info/OEMC_Private_Sect_Fact_sheet.pdf

KEY WORDS: CCTV, security cameras, video interoperability, video security systems, situational awareness systems, incident command

TECHNICAL POINT OF CONTACT: Marilyn Rudzinsky, 202-254-2328, marilyn.rudzinsky@hq.dhs.gov

---

SBIR TOPIC NUMBER: H-SB016.1-002

TITLE: Applicability of Blockchain Technology to Privacy Respecting Identity Management

TECHNOLOGY AREAS: Identity, Privacy, and Cybersecurity

OBJECTIVE: Design information security and privacy concepts on the blockchain to support identity management capabilities that increase security and productivity while decreasing costs and security risks for the Homeland Security Enterprise (HSE).

DESCRIPTION: Blockchain technologies, if incorporated with the security and privacy capabilities required by the HSE, potentially offer a flexible, resilient and potentially lower cost alternative to current Homeland Security Enterprise identity management capabilities.

Current HSE identity management deployments utilize centralized authoritative sources to vouch for the accuracy of the information they collect and maintain. While mechanisms for storing this information can vary (Lightweight Directory Access Protocol (LDAP), databases, Active Directory, etc.), they are ultimately a type of organizationally owned and controlled ledger.

This in turn has led to an ecosystem where processing a transaction to validate information (e.g., birth date) it is necessary to (1) first discover the entity that is considered authoritative for that information, (2) establish the technical means (protocols, data formats, etc.) to interact with that entity, and (3) rely upon the ability and scalability of that entity to validate the information.

Potential examples of this type of interaction within the Homeland Security Enterprise (HSE) are validation of employment status, citizenship, eligibility to work, validation of qualifications of first responders and any other type of interaction that requires a central authority to provide a distributed validation capability.

However, recent innovations around crypto-currencies point to a potential answer to this dilemma. Of particular interest is the underlying technology of the 'bitcoin' crypto-currency, which is called the blockchain. The blockchain is in effect a common, public ledger, which utilizes cryptographic mechanisms to verify transactions and information in a decentralized manner.

The potential applicability of blockchain technology goes beyond crypto-currencies (which is simply an application built on top of that technology) to many other uses such as smart contracts, provenance and attribution, distributed validation of information and more.

This SBIR topic is focused on determining and demonstrating if classic information security concepts such as confidentiality, integrity, availability, non-repudiation and provenance as well as privacy concepts such as pseudonymity and selective disclosure of information can be built on top of the blockchain to provide a distributed, scalable approach to privacy respecting identity management.

PHASE I: Analyze the current implementation of the public blockchain technology and develop the concepts and methods needed to demonstrate the implementation of information security principles of confidentiality, integrity, availability, non-repudiation and provenance as well as

privacy concepts such as pseudonymity and selective disclosure of information on the public blockchain.

This phase will demonstrate the various information security and privacy concepts and methods using a multi-user information-sharing prototype and provide detailed architecture and technical details that document and explain the implementation. In addition, this phase will explore, analyze and document the feasibility of applying the developed concepts and methods to a private or consortium based blockchain.

PHASE II: Apply the concepts and methods developed in Phase I to the domain of identity management – in particular to the assertion and validation of identity information (i.e., attributes).

Phase II will demonstrate via a prototype how such a system could interoperate with existing identity assertion, validation and attribute sharing infrastructure built on top of current protocols such as SAML 2, OpenID Connect and OAUTH2. It will provide detailed architectural papers, technical details and prototype code that explain and document the implementation. In addition, this phase will explore, analyze and provide documentation on the incentive structures that need to be put into place for the adoption of this technology over the status quo.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: Potential HSE Applications of this technology include attribute registries used to share emergency responder qualifications, employment eligibility or organizational affiliations as a precursor to physical and logical access control.

Commercial applications include digital contracts, attribution of knowledge work and more.

REFERENCES:

Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

Buterin, Vitalik. (August 7, 2015). On Public and Private Blockchains. Retrieved from https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

Gault, Mike. (July 5, 2015). Forget Bitcoin — What Is the Blockchain and Why Should You Care? Retrieved from http://recode.net/2015/07/05/forget-bitcoin-what-is-the-blockchain-and-why-should-you-care/

Security Assertion Markup Language v2 (SDO: OASIS), Retrieved from https://www.oasis-open.org/standards#samlv2.0

RFC 9749: The OAUTH 2 Authorization Framework (SDO: IETF), Retrieved from https://tools.ietf.org/html/rfc6749

KEY WORDS: cryptography, bitcoin, blockchain, identity, attributes

TECHNICAL POINT OF CONTACT: Anil John, 202-254-8789, anil.john@hq.dhs.gov

---

SBIR TOPIC NUMBER: H-SB016.1-003

TITLE: Malware Prediction for Situational Understanding and Preemptive Cyber Defense

TECHNOLOGY AREAS: Cyber Security, Cyber Attack Modeling, Resilient Systems, Situational Awareness, Situational Understanding

OBJECTIVE: Develop predictive malware capability and demonstrate a cyber defense method that uses prediction of malware developments to support situational understanding and defensive actions

DESCRIPTION: Situational Understanding for Cyber Security is in its infancy. Although many tools and methods exist, breaches and compromises are in the news almost daily, showing that the current state-of-the-art is ineffective. Hundreds of thousands of unique malware samples are collected on a daily basis. With this onslaught of malware, new defensive techniques must be developed. Predicting malware capabilities and malware development would greatly enhance the situational understanding of cyber defenders. Response to attacks typically occurs only after infiltration or infection of a system. Therefore, the defenders are lagging behind the adversaries, granting attackers a window of success before defensive actions are executed. Preemptive cyber defense, in which the defender is anticipating the next attack rather than responding to the previous one, can shift the advantage away from the attacker and on to the defender. As a result, situational understanding is enhanced and cyber defense is improved because attacks are less effective.

Malware-based attacks are a significant concern to cyber security. Currently, signature-based detection approaches fail to capture novel malware variants, and are not timely, as signatures take days to months to develop. Available detection techniques based on machine learning are limited because they are trained on existing sets of malware. Preemptive defense can address these shortcomings by anticipating what the adversaries will do next. Attacks can be reduced by identifying trends in malware development and predicting them over time. Preemptive malware defense requires an effective capability to predict future malware developments and to exploit these predictions for situational understanding and to improve security.

This SBIR topic seeks methods of predicting malware developments, as well as ways of using these predictions to enhance situational understanding and support malware defense. Predictions which are verifiably correct are paramount to the success of the proposed effort. Thus, meaningful ways of evaluating the predictions should be defined. Emphasis should also be placed on how the proposed techniques can be used to enhance situational understand and as part of a malware defense system.

PHASE I: Design a preemptive cyber defense method capable of identifying trends in malware and predicting malware developments, identify ways of validating this method, and describe how it would be used for enhanced situational understanding and in a defense system.

PHASE II: Create a prototype by implementing the proposed method in a malware defense system that uses prediction of malware developments to improve situational understanding and cyber defense. Specify at least three appropriate metrics, then validate the prototype with these metrics.

Deliverables for Phase II include validation results of the prototype, delivery of a prototype suitable for pilot implementation in a real world setting with metrics showing enhanced situational understanding, success of predictive malware efforts, and success of a preemptive cyber defense method. In addition, there is a requirement to deliver a plan for Phase III.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: This technology will have application in cyber defense efforts of the Homeland Security Enterprise (HSE), and on the commercial market through licensing to software security firms, online providers of software (i.e., application stores), and Government IT providers.

REFERENCES:

Blanch, Rick, “Malware Threats, Trend and Predictions for 2014”, McAfee, 2014

Pfeffer, Avi, et al. "Malware Analysis and Attribution Using Genetic Information." Malicious and Unwanted Software (MALWARE), 2012 7th International Conference on. IEEE, 2012.

Canzanese, Raymond, Moshe Kam, and Spiros Mancoridis. "Toward an Automatic, Online Behavioral Malware Classification System." Self-Adaptive and Self-Organizing Systems (SASO), 2013 IEEE 7th International Conference on. IEEE, 2013.

Neugschwandtner, Matthias, et al. "Forecast: skimming off the Malware Cream." Proceedings of the 27th Annual Computer Security Applications Conference. ACM, 2011

Our top 10 predictions for security threats in 2015 and beyond. (November 12, 2014). Retrieved from: http://www.sophos.com/en-us/threat-center/security-threat-report.aspx

KEY WORDS: Cyber Security, Cyber Attack Modeling, Resilient Systems, Situational Awareness, Situational Understanding, predictive analysis, malware analysis

TECHNICAL POINT OF CONTACT: Ann Cox, 202-254-6198, Ann.Cox@hq.dhs.gov

---

SBIR TOPIC NUMBER: H-SB016.1-004

TITLE: Autonomous Indoor Navigation and Tracking of First Responders

TECHNOLOGY AREAS: Communications, Interoperability, Emergency Preparedness, Response, Community Resiliency, Smart Devices, Wearables

OBJECTIVE: Develop a wearable capability for autonomous indoor navigation and tracking of first responders indoors in various types of building structures.

DESCRIPTION: The S&T First Responders Group (FRG) is devoted to meeting the needs of the first responder community. FRG supports the community's ability to protect the homeland and respond to disasters by ensuring that they have the equipment, technology, and information they need. This involves leveraging a wide array of innovative thinkers and ideas through a variety of vehicles. The DHS S&T Next Generation First Responder (NGFR) program is designing new technologies and leveraging existing capabilities to solve first responder problems and make them better protected, connected, and fully aware. As part of NGFR, this SBIR topic is targeted at meeting a critical need that previous research and development efforts have not been able to achieve: accurately tracking first responders indoors.

The development of sensors and communications able to perform well across a variety of indoor environments is one of the biggest challenges in first responder tracking research and development. The ability to use a Global Positioning System (GPS) is extremely limiting for indoor tracking capabilities due to its weak signal strength and its inability to penetrate buildings. There are limited alternatives to GPS, such as wave measurements, magnetic fields, sonar/acoustics, etc. Each alternative comes with both benefits and limitations, and offer varying levels of tracking capability. Previous research and development activities have highlighted the significant challenges associated with indoor tracking. In early 2015, the Federal Communications Commission (FCC) provided rules to ensure commercial cellular carriers and equipment vendors can come together to field more accurate indoor 911 wireless caller, (i.e., cell phone), location capabilities (see reference #1 and #2 below) to enable First Responders to derive a "dispatch-able" address based on the location of the cellular telephone. In a similar context, FRG is seeking personalized, modular and scalable approaches to track next generation first responders indoors using current or emerging technologies, sensors, and techniques. The proposed technology must work regardless of materials used in the building structure, (e.g., wood, concrete, steel, glass or any combination of building materials), and of varying heights. Ideally, a solution will be wearable, self-reporting, provide real-time x, y, z positioning, and will be mission agnostic allowing for use with any first responder practitioner (e.g., law enforcement, firefighter, emergency management, etc.).

PHASE I: Develop a high level concept of operations for a next-generation indoor tracking capability that includes: a listing of the various connected wearable sensors and tools targeted, as well as relevant first responder use cases for their application. The concept of operations for this tracking capability shall include a conceptual, scalable, next-generation architecture that supports multiple communications networks (e.g., Land Mobile Radio (LMR), Commercial as well as Public Safety Broadband, Satellite, Long-Term Evolution (LTE) deployable, Wi-Fi, etc.) connected to existing and theoretical first responder devices. It shall also embrace a standards-based approach (e.g., Open Geospatial Consortium, BlueTooth, Zigby). Finally, the concept of

operations shall also include a section outlining the technical feasibility and potential first responder operational improvement areas.

Deliverables include; monthly quad chart that shows task descriptions, percentage completed, targeted completion date, etc.; monthly status calls to discuss the monthly technical report and quad chart.

PHASE II: Based off of work completed in Phase I, develop a detailed next-generation technical architecture. The architecture must identify and propose relevant standards, and interfaces. The offeror must also develop and deliver a minimum of four, or more, working prototypes and conduct trials to evaluate the operational use of the proof of concept based on Phase I use cases. A comprehensive security assessment must also be provided.

Additional deliverables in Phase II include; monthly quad chart that shows task descriptions, percentage completed, targeted completion date, etc.; monthly status calls to discuss the monthly technical report and quad chart.

Finally, there is a requirement to assist DHS S&T Communications, Outreach and Responder Education (CORE) personnel in the development and review of communications materials.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: Based on the results of the Phase II trials, there is potential for this technology to be inserted into S&T's NGFR program and Customs and Border Protection (CBP) agents needing tracking capabilities while operating indoors.

This technology could also be leveraged by the commercial sector in market segments where people or objects need to be tracked indoors, and by wireless carriers to support FCC Wireless E911 Location Accuracy Requirements.

REFERENCES:

FCC Wireless E911 Location Accuracy Requirements, PS Docket No. 07-114 (March 3, 2015). Retrieved from: https://www.fcc.gov/document/fcc-adopts-new-wireless-indoor-e911-location-accuracy-requirements-0

Cellular Carriers Technology Roadmap and Wireless E9-1-1 Location Accuracy Requirements (January 21, 2015). Retrieved from: http://apps.fcc.gov/ecfs/comment/view?id=60001009867

Project Responder 4: 2014 National Technology Plan for Emergency Response to Catastrophic Incidents (July 2014), Homeland Security Studies and Analysis Institute. Retrieved from: http://www.firstresponder.gov/TechnologyDocuments/Project%20Responder%204.pdf

KEY WORDS: indoor location, situational awareness, indoor 3D map, RF ranging, barometric altimeter, velocimeter, inertial measurement.

TECHNICAL POINT OF CONTACT: Sridhar Kowdley, 202-254-8804, Sridhar.Kowdley@hq.dhs.gov

---

SBIR TOPIC NUMBER: H-SB016.1-005

TITLE: Internet of Things (IoT) Low-Cost Flood Inundation Sensor

TECHNOLOGY AREAS: Flood Resilient Communities; Information Sharing; Interoperable Communications; Wireless Emergency Alerts; Alerts (WEA); Warnings and Notifications; Deployables; Internet of Things (IoT); Sensor Web Enablement; Mesh Network

OBJECTIVE: Develop deployable, low-cost flood inundation sensor for alerts, warnings and notifications to responders and citizens using IoT Wireless Emergency Alerts

DESCRIPTION: Flooding is the nation's leading natural disaster accounting for the greatest loss of life, property damage, and environmental degradation. Man-made discharge from hydroelectric power supplies, while a controlled release, can result in life-threatening situations as the stage/discharge downstream impacts recreational, residential and commercial properties and people. Flash flooding can result in rapid inundation of low-lying areas, underpasses, and critical transportation corridors—impacting emergency response, isolating critical infrastructure, and posing life-threatening situations. The ability to rapidly predict, detect and react to ever-changing flood conditions requires the ability to monitor flood-prone areas in real-time across large geographies.

Providing flood monitoring across broad areas requires a scalable mesh network of affordable, interoperable sensors. The ability to accurately predict and project the rise of flood waters requires the design and development of a ruggedized, modular, deployable (attached to natural or man-made physical structures), GPS-enabled (x, y and z), submersible, low-cost flood sensor; it must also have a wireless, sustainable power source that operates based upon open, web-enabled sensor standards that can leverage an open source IoT architecture design. The flood sensors, and their associated mesh network, would first relay information through open data exchange standards for inclusion within an organization's operation center for analysis. From there, information would relay to hand-held devices through wireless emergency alerting and then to other IoT sensors for detection and verification.

The resulting IoT Flood Inundation Sensor is expected to be designed and developed in such a way to facilitate its commercialization at a commodity-based level to allow procurement and adoption by rural, resource-constrained communities in the United States and around the world.

PHASE I: Prepare an engineering concept report for the design of a modular, low-cost, integrated flood inundation sensor(s) that meets all of the requirements in the description, based upon both best available technology and best affordable technology. The sensor design will be based on current state of the technology as well as based on requirements derived from DHS S&T

stakeholder community, including the Lower Colorado River Authority (LCRA) and the Texas Department of Public Safety (TDPS).

Deliverables include; engineering concept report that includes initial schematic design, modular sensor engineering specifications, functional characteristics, performance and operational parameters and target unit cost estimations; monthly quad chart that shows task descriptions, percentage completed, targeted completion date, etc.; monthly status calls to discuss technical report and quad chart.

PHASE II: Develop, deploy, test, evaluate, and monitor a prototype of an IoT low-cost flood inundation sensor(s) mesh network, consisting of a minimum of 100 viable sensor units, based upon the engineering concept report design criteria and user requirements from Phase I. Part of the Phase II effort will be to engage the DHS stakeholders (e.g., LCRA and TDPS) to determine the mesh network deployment, evaluation and performance testing acceptance criteria. The assembled sensors, and the associated application programming interfaces (APIs) necessary to implement the mesh network protocols, will be provided to and integrated with the stakeholder operational centers to perform the operational test and evaluation. The test and evaluation should be performed no later than the 18th month of the contract period of performance, over a period of not less than 4 months to align with the regions annual flooding periods. The DHS stakeholders will provide in-kind services, access to subject matter experts, operation center and other architecture environments necessary to deploy, test and monitor the sensor network deployment and operation.

Phase II deliverables shall include; kick-off meeting; monthly quad chart that shows task descriptions, percentage completed, targeted completion date, etc.; monthly status calls to discuss technical report and quad chart; a minimum of 100 viable sensors, associated APIs and necessary software for implementation, technical implementation guidance, test and evaluation plans, and six (6) months of sensor monitoring and diagnostics for sensor performance. Performance and evaluation criteria will be co-developed with S&T and stakeholders. In addition, there is a requirement to deliver an engineering findings report for repeatable, scalable commercialization of the IoT Flood Inundation Sensor network toward the end of the performance period.

Finally, there is a requirement to assist DHS S&T Communications, Outreach and Responder Education (CORE) personnel in the development and review of communications materials.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: Several flood sensor initiatives highlight the need for early warning for flooding, especially in developing countries. However, even the United States has yet to develop and commercialize a low-cost flood alert, warning and notification sensor capability to address the nation's most common and costly hazard. Over the last 30 years, the average losses from flood events have been 89 fatalities and $8.2 billion in damages per year.

The DHS stakeholders involved in this initiative (e.g. LCRA and TDPS) have indicated their interest in deploying a comprehensive mesh network array across their jurisdictional areas of responsibility.

In addition to this homeland security application for flood resiliency and response, other homeland security and commercial applications for open standards-based, modular components could be designed and used toward the following government missions and commercial services: audio and visual alerts, reverse 9-1-1, road closure routing, onboard transceiver and service applications, and a number of smart city and smart transportation services as an IoT offering.

REFERENCES:

Autonomous Field-Deployable Wildland Fire Sensors. (2003). Retrieved from: http://www.researchgate.net/publication/245577508_Autonomous_Field-Deployable_Wildland_Fire_Sensors

Cheap Deployable Networked Sensors for Environmental Use. (December 2014). Retrieved from: http://telsoc.org/ajtde/2014-12-v2-n4/a62

Project Responder 4: 2014 National Technology Plan for Emergency Response to Catastrophic Incidents (July 2014), Homeland Security Studies and Analysis Institute. Retrieved from: http://www.firstresponder.gov/TechnologyDocuments/Project%20Responder%204.pdf.

Lower Colorado River Authority (LCRA) Interactive Map: http://maps.lcra.org/interactive.aspx

KEY WORDS: Flood, Internet of Things, Smart City, Open Web Standards, Sensor Web Enablement (SWE); First Responder Early Warning, Resilience; Mesh Network

TECHNICAL POINT OF CONTACT: Jeff Booth, 202-254-6347, Jeffrey.booth@hq.dhs.gov

---

SBIR TOPIC NUMBER: H-SB016.1-006

TITLE: Low-Cost, Real-Time Data Analytics for Underserved EMS Agencies

TECHNOLOGY AREAS: Communications, predictive (data) analytics, information sharing, incident response and management, operational framework, real-time incident management.

OBJECTIVE: A low-cost, real-time data analytics solution to enable underserved Emergency Medical Service (EMS) and first responder agencies to improve quality and response

DESCRIPTION: While the United States has a National emergency call system, there is no national standard on how these calls are recorded, reported or stored when someone calls 9-1-1.

Without a standard, communities have selected from a myriad number of Computer Aided Dispatch (CAD) vendors, each with a proprietary software solution and an accompanying set of features and cost models. Not only are there significant differences in the capabilities of these systems, there are different technical architectures, workflows, and use cases. With over 3,100 counties in the United States and no standards, 9-1-1 incident data (as recorded in the CAD databases) can vary from county to county, municipality to municipality, provider to provider and state to state. With such a broad and disparate set of technologies supporting CAD, EMS and first responder agencies vary in how they provide operational response to these call incidents.

Further, this wide range of solutions comes at various costs; this poses a substantial challenge for agencies that have limited resources. EMS and first responders in many communities do not have new infrastructure, which limits or eliminates access to data. Without current and relevant data, change management processes and continuous quality improvement, which inform and improve response during emergencies, is limited or non-existent.

On the vendor side, a very limited number of real-time analytic solutions exist today and they require considerable integration and maintenance. This requirement further pushes the cost of those solutions beyond the reach of many underserved EMS agencies. This limitation in the marketplace has precluded the ability of underserved EMS agencies to become high performing EMS agencies.

This topic focuses on addressing the need for a low-cost (or no-cost) data analytics solution that can support EMS and first responder agencies irrespective of their resource levels. The solutions needs to be low-/no- cost, and must operate independent of proprietary or vendor-specific database architectures, and must enable real-time access, analysis and reporting of CAD data.

The DHS First Responders Group envisions this early-stage work under SBIR to lay the groundwork for a broader, innovation that gives thousands of EMS and first responder agencies the opportunity to become high-performance organizations. Consistent with S&T's Visionary Goals of Enabling the Decision-Maker and Protecting the Responder of the Future, this work can also seed longer-term efforts to create a national, standards-based solution that supports real-time or predictive analytics for timely, actionable response information and that can drive de facto reporting standards that will enable regional, statewide and nationwide views of operational incident data.

PHASE I: Identify key performance indicators (KPI) from high performing EMS and first responder agencies in varied geographic and rural versus urban settings. This Phase will establish the feasibility of producing a prototype solution that provides a low cost real-time EMS analytics tool, leveraging the identified KPIs. Included in the final technical report will be an analysis of county attributes in different geographic locations.

Deliverables include; monthly quad chart that shows accomplishments, milestones, activities and risks; monthly status call to discuss the monthly technical report and quad chart; and quarterly

Interim Project Review (IPR) that includes power point presentation on the status of the research, preliminary or expected findings, and any risks associated with work in progress.

PHASE II: Using a subset of KPIs defined in Phase I, develop the data and technical architecture to support a low cost real-time data analytics prototype. Conduct at least two pilots or trials that confirm the operational value of the prototype.

Deliverables in Phase II include; monthly quad chart that shows accomplishments, milestones, activities and risks; monthly status call to discuss the monthly technical report and quad chart; quarterly Interim Project Review (IPR) that include power point presentation on the status of the research, preliminary or expected findings, and any risks associated with work in progress; and completion of a one page template, to be provided by DHS S&T FRG, outlining a communications and outreach for after Phase II (i.e., list of Government agencies that will benefit from technology, outreach events that will provide partnering opportunities, etc.). During Phase II there is a requirement to assist DHS S&T FRG Communications, Outreach and Responder Education (CORE) personnel with the development and review of communications materials.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: Based on the strength of Phase II prototypes and pilots—as well as the strength of a commercialization plan that facilitates adoption—the capabilities that result from this effort will provide the foundation of a real-time data analytics solution which would be available for any US EMS agency as part of their Continuous Quality Improvement (CQI) program.

However, there is significant potential for other state, local and commercial healthcare and emergency medical services segments to take interest in and/or invest in bringing this EMS capability to market if it demonstrates the potential to influence efficiencies and outcomes for emergency medical care facilities and professionals.

REFERENCES:

Lawrence, R. (January 1, 2015). 10 Tips to Stay on Top of Your EMS Game. Retrieved from EMSWorld: http://www.emsworld.com/article/12026076/10-tips-to-stay-on-top-of-your-ems-game

Lim, C. S., Mamat, R., & Braunl, T. (June 2011). Impact of Ambulance Dispatch Policies on Performance of Emergency Medical Services. Retrieved from: http://www.therevproject.com/publications/uwa/J2011-IEEE-Impact%20of%20Ambulance%20Dispatch%20Policies%20on%20Performance%20of%20Emergency%20Medical%20Services-Lim%20Mamat%20Braunl.pdf

KEY WORDS: Emergency call system, standards adoption, quality improvement, computer-aided dispatch (CAD), incident response, technology standards.

TECHNICAL POINT OF CONTACT: Denis Gusty, 202-254-5647, denis.gusty@hq.dhs.gov

---

SBIR TOPIC NUMBER: H-SB016.1-007

TITLE: Real-Time Assessment of Resilience and Preparedness

TECHNOLOGY AREAS: Community, Economic & Infrastructure Resilience; Emergency Preparedness and Response; Natural Disasters and Related Geophysical Studies; Advanced Data Analysis and Visualization; and Communications & Interoperability

OBJECTIVE: Develop an application to assess a community's posture with respect to resilience factors (to be provided by the government) using open-source data streams such as print and visual media, government data bases, and social media.

DESCRIPTION: Communities across the United States are in different states of preparedness for a natural disaster. Assessing a community's resilience requires a dedicated, expensive, and time-consuming data collection effort and produces information that quickly becomes outdated due to ongoing changes in the community. For example, community planners may invest in a new road construction that would influence a community's resilience factor, but was not captured in the initial data collection. Essentially, evaluating a community's resilience using existing methods and technology yields a static 'snapshot', which, while useful in the near term, is not sufficient to inform federal, state, and local disaster planning efforts.

There is a need for a low-cost, flexible application that can analyze a community's resilience on a near real-time basis and present this information in visual and data formats on mobile and fixed platforms. The application would access open-source data feeds, such as print and visual media, social media, and community and state government data, and use this information to evaluate a community's preparedness using DHS-provided resilience factors.

Technical challenges involve the identification of open-source data that are relevant to DHS-provided resilience factors and the development of algorithms to analyze and prioritize these data against the resilience factors. The application must be able to incorporate new data in real time to support an accurate assessment of a community's resilience state. In addition, the application must be engineered for deployment on smart phones, tablets, and PC platforms.

PHASE I: Develop a program plan that outlines the overall system architecture and technology required to develop the resilience assessment application. The architecture will specifically identify the targeted open-source data to be used and how the data will be analyzed and displayed to a user. Include milestones, description of demonstrations, and a comprehensive technical description of the developed application.

PHASE II: Develop an application that uses open-source data to assess a community's resilience and provides results to a user. Test the application's effectiveness in providing accurate

resilience information (DHS will provide the community and specific disaster of interest six months after the start of Phase II) and provide results of the test.

Provide a comprehensive business plan to make the application commercially available to community, state, commercial, and federal planners.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: This technology can strengthen disaster preparedness and response for government entities such as the Federal Emergency Management Agency (FEMA) and the Department of Commerce, as well as State and local governments, commercial insurance firms, and the construction, medical, and foodstuff industries. The data provided through this application will assist community planners and support government and private sector decision-making before, during, and after a disaster.

REFERENCES:

Fine Maron, Dina. (June 7, 2013). How Social Media Is Changing Disaster Response. Retrieved from http://www.scientificamerican.com/article/how-social-media-is-changing-disaster-response/

Zumbrun, Josh. (August 24, 2015). Economic Forecasting Is Getting More Up-to-the-Minute. Retrieved from http://www.wsj.com/articles/economic-forecasting-is-getting-more-up-to-the-minute-1440456255

KEY WORDS: Information Collection, Information Management, Collaborative Analysis, Collaborative Decision-making, Social Understanding, Cultural Understanding, Behavioral Understanding

TECHNICAL POINT OF CONTACT: Erin Walsh, 202-254-8248, erin.walsh@hq.dhs.gov

---

SBIR TOPIC NUMBER: H-SB016.1-008

TITLE: Using Social Media to Support Timely and Targeted Emergency Response Actions

TECHNOLOGY AREAS: Communications, information sharing, technology acquisition, Computer Aided Dispatch (CAD), data analytics, social media, crowd-sourcing

OBJECTIVE: Develop a data analytics engine (set of algorithms) to correlate social media comments and activity with real time agency CAD incident data.

DESCRIPTION: Social media outlets, such as Facebook, Twitter, Instagram, and Snapchat, to name a few, have become ubiquitous in the modern world of communications. During real-world emergency events there potentially exists a wealth of unstructured information and unverified datasets about these events that are being shared via social media outlets as the events are

unfolding. Organizing and correlating this information with CAD incident data already available to the Incident Command could greatly improve the effectiveness of response decisions and actions. This crowd-sourced data, once validated (including an analysis of any potential false positives) could be correlated with actual real-time incident data, so that more timely and targeted response actions can be identified that allow for escalation preparedness throughout the event timeline.

Public Safety, Fire and Emergency Medical Services (EMS) agencies generally use CAD data to understand actions occurring in the past. The data is often aggregated around specific quantitative metrics and does not capture broader, influential external factors including environmental, social, meteorological, political, economic, and other factors. The impact of these factors is often only known as part of post-event analysis as they are not a part of the reportable incident data set available in the Computer Aided Dispatch (CAD) system during the event.

Identifying the types of influential external factors—which are often shared via social media—and correlating those factors with CAD information can drive an enhanced, upgraded, or differing response that could impact community preparedness and resilience. The resultant actionable data will support decision making as events unfold (instead of afterward), better; this serves the community as a whole, reduces risk, and ensures the best use of resources.

PHASE I: Develop a target set of scenarios that would benefit from social media correlation. Identify the broader external factors, usually discussed in social media feeds, which can improve situational insight to the target set of scenarios. Identify the operational incident (CAD) data that correlates with the social media feeds for the target set of scenarios. Describe the technical feasibility of developing algorithms to correlate social media with incident command data feeds for the target set of scenarios and the potential improvements in real-time/response operations.

Deliverables include; monthly quad chart that shows accomplishments, milestones, activities and risks; monthly status call to discuss the monthly technical report and quad chart; and quarterly Interim Project Review (IPR) that includes power point presentation on the status of the research, preliminary or expected findings, and any risks associated with work in progress.

PHASE II: Down select to a single target scenario based on Phase I and development of the set of algorithms to support a pilot protocol by which a social media feed is correlated with operational incident data. Establish the validation and trust algorithms that could support more timely and targeted response actions and allow for escalation preparedness.

Deliverables in Phase II include; monthly quad chart that shows accomplishments, milestones, activities and risks; monthly status calls to discuss the monthly technical report and quad chart; quarterly interim project briefings (IPR) that include power point presentation on the status of research, preliminary or expected findings, and risks associated with the work in progress; and

completion of a one page template, to be provided by DHS S&T FRG, outlining a communications and outreach plan for after Phase II (i.e., list of Government agencies that will benefit from technology, outreach events that will provide partnering opportunities, etc.). During Phase II there is a requirement to assist DHS S&T FRG Communications, Outreach and Responder Education (CORE) personnel with the development and review of communications materials.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: Based on the results of the Phase II technology, an integral standardized output format would be developed, which would post correlated results to a web dashboard for use by local Public Safety officials and 9-1-1 communications dispatchers. Once standardized, a national view of scenarios could then be used by DHS to understand local, regional and state incident data as correlated with social media to better understand risk scenarios that could impact the United States as a whole, or individual states or regions.

REFERENCES:

Wang, Dashun, Lin, Yu-Ru , & Bagrow, James P. (2012). Social Networks in Emergency Response. Retrieved from http://bagrow.com/pdf/2012-emergbook.pdf

Dillow, Chris. (March 25, 2014). Do social media distort financial decision making? Retrieved from http://www.ezonomics.com/blogs/its_possible_that_social_media_have_at_least_one_downside_they_can_distort

Shklovski, Irina & Latonero, Mark. (2011, Oct-Dec). "Emergency Management, Twitter,and Social Media Evangelism." Retrieved from www.acedemia.edu: http://www.academia.edu/1071890/Emergency_Management_Twitter_and_Social_Media_Evangelism

DiMauro, Vanessa. (November 2009). Traditional Decision-Making Process is Disrupted By Social Media. Retrieved from http://www.leadernetworks.com/2009/11/traditional-decision-making-process-is.html

IBM Corporation. (February 2013). Integrating social media and advanced analytics for richer customer insight. Retrieved from IBM Briefing Paper: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=SP&appname=SWGE_YT_YT_USEN&htmlfid=YTS03027USEN&attachment=YTS03027USEN.PDF

KEY WORDS: Social media, social networks, crowd-sourcing, computer-aided-dispatch (CAD), technology integration, 9-1-1 dispatch, incident response.

TECHNICAL POINT OF CONTACT: Denis Gusty, 202-254-5647, denis.gusty@hq.dhs.gov

SBIR TOPIC NUMBER: H-SB016.1-009

TITLE: Blockchain Applications for Homeland Security Analytics

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

OBJECTIVE: Design a product to support the implementation of block chain based data management, data analysis, and information sharing.

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 in crypto currency, known as 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.

PHASE I: Design and prototype an ecosystem that supports blockchain technology applications for data analytics that significantly improve DHS mission and operations. Proposed use cases include, but are not limited to, crypto-certified data and/or analytic transactions involving users and devices for the internet-of-things applications (IoT) such as encrypted sensor data transactions and analytics for first responders; information sharing and analysis between state, local, and federal law enforcement; and third party information sharing architectures involvement, perhaps in applications that improve security and experiences for the traveling public, or that improve bio-threat awareness. Offerors may define and propose relevant use cases and architectural concepts where there is a significant value proposition for the homeland security enterprise.

Proposed solutions can involve open or closed environment blockchain applications. For example, open environments, such as cryptocurrencies, where anyone can participate. There are also closed-permissions based environments where community involvement may be controlled by participants. 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, network and information security policies and standards are also important considerations for a viable solution that involves government participation. For scalability, solutions must also consider speed of analysis and any transaction validation features.

In Phase I, the application ecosystem will be developed for data management that will include a data 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 where practicable; show how components and services function in the ecosystem; and develop an approach for building and maintaining this ecosystem. Demonstrate and/or document implementation feasibility with respect to: concept of operations, crypto-certified data transactions, governance models, analytic framework, analytic algorithms, costs, privacy protection and security. Identify risks to privacy, security, operational performance and technology and develop appropriate risk mitigation strategies.

PHASE II: Prototype, or expand on the prototype, developed in Phase I for the blockchain data management ecosystem(s), including the development of software services and design, and implementation of any equipment needed. Implement, expand, refine and characterize the performance of 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 the value proposition of 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. Initiate transition/commercialization options that leverage the strengths of demonstrated results, market demand and homeland security value propositions.

In Phase II, the software ecosystem prototype will be delivered and made available to the government for assessment. This can happen through the delivery of preliminary software, equipment, or cloud based platform access.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: Blockchain technologies stand to radically transform options for data management, sharing and analysis across government. Because of the significant impact in areas such as governance, data sharing agreement enforcement, and encrypted analytics interchanges, there are a wide variety of applications in government and the commercial marketplace that can benefit from successful product development. Information sharing for the homeland security enterprise can help the DHS security operations across components as well as the state fusion centers. Additionally, such technologies can assist with resolving matters related to disaster response, where a variety of

public and private resources are required to inform decision making at all levels of government and for individuals.

REFERENCES:

Maras, Elliot. (May 9, 2015). MIT Digital Currency Initiative Leader to Government Officials: Let's Get 'Open Data 2.0 Moving'. Retrieved from https://www.cryptocoinsnews.com/mit-digital-currency-initiative-leader-government-officials-lets-get-open-data-2-0-moving/

Hayase, Nozomi. (October 14, 2014). How Bitcoin's Block Chain Could Stop History Being Rewritten. Retrieved from http://www.coindesk.com/block-chain-aid-fight-free-speech/

Hayase, Nozomi. (November 22, 2014). The Blockchain and the Rise of Networked Trust. Retrieved from http://www.coindesk.com/blockchain-rise-networked-trust/

Device democracy – Saving the future of the Internet of Things. Retrieved from http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=XB&htmlfid=GBE03620USEN

Orcutt, Mike. (July 9, 2015). Why Nasdaq Is Betting on Bitcoin's Blockchain. Retrieved from http://www.technologyreview.com/news/539171/why-nasdaq-is-betting-on-bitcoins-blockchain/

KEY WORDS: Identity, encryption, crypto-certification, encrypted data analytics, authentication, cyber security, internet of things, and data analytics

TECHNICAL POINT OF CONTACT: Stephen Dennis, 202-254-45788, Stephen.Dennis@hq.dhs.gov

---

SBIR TOPIC NUMBER: H-SB016.1-010

TITLE: Remote Identity Proofing Alternatives to Knowledge Based Authentication/ Verification

TECHNOLOGY AREAS: Identity, Fraud, and Cybersecurity

OBJECTIVE: Design and demonstrate the feasibility of high assurance alternatives to knowledge-based verification techniques for population scale remote identity proofing.

DESCRIPTION: The vast majority of organizations remotely identity proof an individual using a Knowledge Based Verification (KBV) or Knowledge Based Authentication (KBA) technique; i.e., by asking them "secret" questions that only they can supposedly answer to prove their identity.

As shown by the recent Internal Revenue Service (IRS) data breach, KBV is broken and rapidly becoming less effective as a verification tool as a by-product of the availability of personal

information on social media as well as the variety of data breaches of credit bureaus and data brokers. This availability of personal information has led to situations where answers to these "secret" questions can easily be discovered with a minimal level of effort by a determined fraudster who can then use that information to impersonate an individual.

At a high level, identity proofing of an individual is a three step process consisting of (1.) identity resolution (confirmation that an identity has been resolved to a unique individual within a particular context, i.e., no other individual has the same set of attributes), (2.) identity validation (confirmation of the accuracy of the identity as established by an authoritative source) and, (3.) identity verification (confirmation that the identity is claimed by the rightful individual).

This SBIR topic is focused on investigating identity verification alternatives to KBV/KBA that provide varying levels of assurances of identity for remote identity proofing. Potential techniques to be explored include, but are not limited to, biological or behavioral characteristic confirmation - a process that compares biological (anatomical and physiological) characteristics in order to establish a link to an individual where facial photo comparison, trusted referee confirmation - a process that relies on a trusted referee to establish a link to an individual (guarantors, notaries and certified agents are examples of trusted referees), and physical possession confirmation - a process that requires physical possession or presentation of evidence to establish an individual's identity.

PHASE I: Identify and define five or more non-KBV/KBA approaches that exist in practice and in theory to establish a link between a particular set of data and an individual. Perform an analysis to determine the technical feasibility of each approach as well as the threats and potential mitigations for each approach.

PHASE II: Analyze and rank the approaches, or combination of approaches, identified in Phase I based on the assurances of identity they provide.

In addition, to the extent feasible, provide a mapping to the levels of identity assurances as articulated by standards organizations such as International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST). Provide an analysis of the various approaches that take into account identity assurance, data privacy, and user experience. Using data from the analysis, develop, demonstrate, and validate the most promising approaches that provide the best combination of identity assurance, privacy and user experience via a prototype using existing standardized identity protocols such as Security Assertion Markup Language 2.0 (SAML 2.0) or OpenID Connect / OAUTH2.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: Potential Homeland Security Enterprise (HSE) Applications of this technology include all digital services delivered by government to its citizens, employees or partners that require remote identity proofing.

Commercial applications include all high assurance applications requiring proof of identity.

REFERENCES:

Office of Management and Budget. E-Authentication Guidance for Federal Agencies (OMB-M-O4-O4) http://csrc.nist.gov/drivers/documents/m04-04.pdf

NIST, Electronic Authentication Guideline (NIST SP-800-63-2) http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

ISO/IEC 29115: Information technology -- Security techniques -- Entity authentication assurance framework http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45138

IRS Statement on the "Get Transcript" Application. (May 26, 2015). Retrieved from: https://www.irs.gov/uac/Newsroom/IRS-Statement-on-the-Get-Transcript-Application

KEY WORDS: identity, proofing, Knowledge Based Verification, KBV, Biometrics

TECHNICAL POINT OF CONTACT: Anil John, 202-254-8789, anil.john@hq.dhs.gov

---

SBIR TOPIC NUMBER: H-SB016.1-011

TITLE: Smartphone/Smart device Toolkit for Virtual and Actual Radiation Detection, Identification, and Localization

TECHNOLOGY AREAS: Radiation Detection; Virtual Radionuclide Identification; Localization, Human-machine interface, Instrumentation, Human Factors, Psychology, Display systems

OBJECTIVE: Successful research would lead to the development and demonstration of a user-friendly and straightforward smartphone/smart device toolkit for radiation detection, identification, and localization based on the presence of a simulated or virtual radiological source. Later phase device will be able to interface with actual detector to provide same functionality using data generated by detector resulting in near-perfect fidelity between training and operations.

DESCRIPTION: DNDO is requesting proposals that lead to the development of a simple-to-use and operate radiation source training and operational toolkit that contains the following:

- A display output with design developed from basic research (survey, observation, SME input) into user needs during actual operational use of fielded instruments. Initial phase will result in optimum user-centered interface responding to a virtual source. Later phase will result in identical interface responding to actual data received from PRD, basic hand held and back pack style detectors.
- Display will have a virtual and active mode.
- Display may be able to either fit over current instrument hardware or be able to be injected directly into hardware.
- Tool is able to track the location of the search personnel compared to the placement of the virtual source for purposes of estimating the detector response, such as through Bluetooth beacons, Wi-Fi, or other equivalent means.
- Selectable ability to change the detector readout types and sensitivity for the purposes of training on multiple detection equipment.
- Output includes estimates of dose and dose rate.
- Source location, isotopic signature, intensity, and occluding background environment can be programmed for training purposes.
- The application may support several modes of operation within existing detection systems to include detection, localization, and identification.
- Later phase tool able to interface with actual detectors providing identical display with selectable menu based on detector capability using detector generated data.

PHASE I: The Offeror shall provide the basic research into optimum human machine interface. Most useful instrumentation/displays for real-world operations at the State and Local level. Most common information required for most effective warnings. Research shall be used to design instrumentation of user interface/instrument display. Additional research would lead to an innovative virtual mock-up which successfully demonstrates the ability of a smart device application to effectively determine the distance of the user from the virtual source, calculate dose and dose rate, and estimate location, signature, and intensity of a source. Offerors would also deliver a prototype user interface capable of supporting multiple modes of operation as described above. Additionally, the Offeror shall deliver a detailed analysis of predicted performance, establish baseline metrics, and include monthly progress and final technical reports as part of the standard Phase I deliverables.

PHASE II: Phase II efforts shall focus on the validation and verification of simulated results in various operational environments, including those with background occlusion. Further, the Offeror shall be able to demonstrate that the performance of this virtual model exceeds the previously established baseline metrics set forth in Phase I. Efforts should roll into development of digital architecture for app based display that would allow virtual mode interface be duplicated and provide real-time data from actual detectors. The efforts would result in demonstration of a smart device tool that uses same instrumentation as virtual tool, but provides actual detector data. This will lead to the development of open architecture standards for smart device interface with R/N equipment hardware. Open architecture will spawn innovation in turning standard digital data into innovative displays and innovative information transfer solutions that provide near-perfect fidelity between training and operational use.

The end of the second year Phase II efforts should culminate into a robust and standalone smartphone/device app or toolkit, adjustable to emulate detector responses and to interface with actual commonly used detectors (PRD, BHH, Back pack). Display would have selectable features compatible with detector capability standardizing display features for family of commonly used detection equipment.

PHASE III - COMMERCIAL OR GOVERNMENT APPLICATIONS: Efforts should focus on developing partnerships and collaborations with R/N OEMs, other Government, State, and Local emergency response organizations for a successfully transition of the resulting smartphone/device application(s) as a standard all-encompassing equipment solution toolkit to facilitate training, operations and exercises. Developer could commercialize as optimum app based display/ Interface solution that can provide both training and operational functionality. Device could be marketed on near perfect fidelity for training and interface solution that would negate training gaps between commonly used equipment (PRD, Handheld, Back pack). This toolkit could be further expanded to include testing of new and more advanced detection, identification, or localization algorithms developed by DHS research and development efforts. This toolkit could be further expanded to include additional advanced human machine interfaces to support operational constraints.

REFERENCES:
http://www.infoworld.com/article/2608498/mobile-apps/what-you-need-to-know-about-using-bluetooth-beacons.html

KEY WORDS: Virtual; Radiation Source; Smartphone Toolkit; Detection; Identification; Tracking; Localization

TECHNICAL POINT OF CONTACT: fy16dndosbirquestions@hq.dhs.gov

SBIR TOPIC NUMBER: H-SB016.1-012

TITLE: Plastic Composite Based Scintillators for Multi-Signature Radiation Detectors

TECHNOLOGY AREAS: Radiation detection, radionuclide identification, plastic scintillators

OBJECTIVE: Demonstrate a simple-to-fabricate-and-integrate detector technology that combines gamma and neutron sensitivity with good efficiency at a reduced cost compare to the current COTS scintillators.

DESCRIPTION: There are considerable benefits in being able to acquire multiple signatures when detecting and identifying radiation sources. While gamma rays can provide highly detailed information alone, they can also be easily masked and misconstrued amongst the many possible sources of industrial, medical and normally occurring sources that might be encountered. For this reason, augmenting with neutron detection is highly valuable, especially in determining the

presence of fissionable materials (SNM). Characterizing neutrons by energy is even more powerful, but often requiring distinctly different detector types.

Recent advances in scintillator technology (*e.g.* elpasolite, stilbene-based, or advanced plastic detectors) make possible both gamma and thermal neutron detection with a single element. The sensor material cost is a significant driver of the overall detector cost, therefore a 'multi-mode' detector approach can shall provide significant value for its enhanced performance. Nevertheless, these new technologies are relatively expensive for wide-spread deployment.

DNDO seeks plastic-crystal composite solutions that can achieve both multi-modality and substantial cost reductions in sensors that are compatible with backpack and handheld instrumentation. Included in the cost calculation is not only the cost to fabricate the scintillator crystals or plastics, but the cost of integrating these gamma/neutron sensitive materials into a detector.

Proposed composite scintillators shall include, but are not limited to a plastic framework comprised of another radiation sensitive material (larger than molecular scale) distributed into the plastic contributing to multi-modality detector sensitivity. The proposal should address the following objectives:

- Price goals should be $\$5/cm^3$ or less.
- Neutron-gamma discrimination should exceed 10^{-6}.
- Gamma ray detection performance shall be better than 1" x 1" NaI single scintillators (7% energy resolution FWHM at 662 keV).

Successful solutions shall leverage the cost effective approach and enhanced detector performance of a combined plastic and radiation sensitive material into a plastic-crystal composite. The most successful technology will provide a compelling combination of gamma ray energy spectroscopy (measured at 662 keV), gamma ray and neutron sensitivity, and cost per unit volume.

PHASE I: The Offeror shall propose a plastic-crystal composite material that can demonstrate multi-mode sensitivity to both gamma rays and neutrons (with separable signals, or discrimination). Neutron detection should also be quantified and compared to current commercially available hand held technologies. Provide trade-off studies and modeling of detector sensitivity as a foundation for Phase II development.

Develop a preliminary cost model that describes the Offeror's plan to manufacture the technology and highlight those factors which are most highly impacted by acquisition scale. It is expected that in Phase II, this model will be updated as the underlying processes mature.

PHASE II: Optimize the underlying technologies and demonstrate fully-sized examples of the working detectors. Develop all packaging and ancillary electronics that may be needed to fully evaluate the detectors, including the capability to discriminate signal types (which should be fully

integrated). Produce packaged detector sizes capable of supporting gamma and neutron detection requirements for handheld and backpack systems.

Further investigation on how this technology could be made available for instrumentation to OEMs, including consideration of accompanying readout requirements.

PHASE III - COMMERCIAL OR GOVERNMENT APPLICATIONS: Handheld and backpack multi-mode gamma/fast neutron/ thermal neutron detectors will strongly benefit from this technology, which will allow their mass deployment in homeland security applications. In addition, it can be used in control of nuclear material diversion and proliferation, for accountability of the materials in nuclear facilities, and in safeguards applications. Large area, low cost, gamma-neutron monitoring systems can be also realized.

REFERENCES:

N. D'Olympia, at al "Optimizing Cs2LiYCl6 for fast neutron spectroscopy," NIM A, vol. 694, pp. 140 - 146, 2012.

N Zaitseva, B L. Rupert, I Pawelczak, A Glenn, H. Paul Martinez, L Carman, M Faust, N Cherepy, S Payne, “Plastic Scintillators with efficient neutron/gamma pulse shape discrimination” , Nucl. Instr. Meth. Phys. Res. A 668 (2012) 88 – 93.

J. Glodo, at al, "Cs2LiYCl6:Ce Scintillator for Nuclear Monitoring Applications," IEEE TNS, vol. 56, no. 3, p. 1257, 2009.

KEY WORDS: Radiation detector, gamma rays, neutrons, scintillators, plastic scintillators

TECHNICAL POINT OF CONTACT: fy16dndosbirquestions@hq.dhs.gov

SBIR TOPIC NUMBER: H-SB016.1-013

TITLE: Portable Linear Accelerator (linac) for Active Interrogation Systems for Radiological Gamma Isotope Source Replacement

TECHNOLOGY AREAS: Portable accelerators, portable active interrogation, gamma isotope source replacement

OBJECTIVE: Develop and commercialize a portable accelerator for active interrogation systems and approaches. The portable accelerator shall replace radiological gamma isotope sources currently used for commercial non-medical applications.

DESCRIPTION: In the past few years, Congress and various Government agencies have recognized the problem of orphaned radioactive sources worldwide. Such sources pose a security risk in the form of potential material for a "dirty bomb" or for other illicit applications. DNDO is seeking alternatives to the radioactive gamma sources used in commercial off-the-shelf products such as oil well logging and soil density gauges. The goal is to dramatically reduce the amount of radioactive material in the commercial market in order to improve public safety and prevent the threat of Radiation Dispersion Devices (RDD). Solutions must be able to directly replace commercial sealed sources used in industry and be competitive with size and cost. They must also achieve the full capabilities of existing systems, but not require the use of a radioactive nuclear material. Their size, weight, and power requirements must not be so onerous as to prevent their use under the conditions normally envisioned for the application. Lastly, they must be sufficiently robust to withstand the temperatures, pressures, humidity, vibration, and shock encountered in the typical operating environment for the application. Furthermore, these technologies could also have applicability in other aspects of the DNDO mission to include portable active interrogation systems for detection of shielded Special Nuclear Material (SNM).

DNDO is seeking the development of an accelerator specifically for human portable non-medical industrial applications with further applicability to portable active interrogation systems. The proposed accelerator shall meet the following specifications:

- Weight: < 50 pounds (includes all supporting electronics)
- Volume: < 1 ft^3
- Output energy: ~1 MeV, with preliminary design capable of 4 MeV operation
- Output radiation: ~1 Rad/min
- Other: Battery operation, ruggedized for industrial use, and low cost (<$50K per unit).

The Offeror's proposal shall provide sufficient details on a path towards achieving the accelerator specifications and subsequent integration into a proof-of-concept prototype. Supporting information (design, data, simulation, analytic calculation, references, etc.) must be provided to justify expectations that program has reasonable chance of successfully achieving its goals.

PHASE I: Demonstrate the feasibility of the proposed technical approach with a benchtop prototype or preliminary design. The physics of critical design elements should be well described.

PHASE II: Development will continue with fabrication and testing of a prototype to demonstrate the viability and capabilities of a radioactive gamma source. Feasibility must be clearly demonstrated in the field or a similar environment.

PHASE III - COMMERCIAL OR GOVERNMENT APPLICATIONS: Homeland Security Application: Commercialization of transformational radiological gamma source replacement techniques and accelerators for portable active interrogation systems and further enhancements of technologies. Production of units for commercial sales through manufacturing, partnering, or

licensing for applications such as oil well logging or soil density gauges or portable active interrogation systems.

REFERENCES:

Method and Apparatus for Gamma Ray Well Logging, United States Patent No. 4,524,273, Issued June 18, 1985.

Apparatus and Method for Gamma-Ray determination of Bulk Density of Samples, United States Patent No, 6,492,641, Issued December 10, 2002.

KEY WORDS: Radiation, radiological, radioactive sources, nuclear sources, soil density gauges, oil well logging, Cs-137, Ra-226, or Co-60 replacement, linac, portable accelerator, portable active interrogation

TECHNICAL POINT OF CONTACT: fy16dndosbirquestions@hq.dhs.gov