DHS-FY19-SBIR-PreSolicitation

The Department of Homeland Security (DHS) Small Business Innovation Research (SBIR) Program, comprised of the Science and Technology (S&T) Directorate's SBIR Program and the Countering Weapons of Mass Destruction (CWMD) Office SBIR Program, invites small business concerns to review this pre-solicitation notice, which is intended to lead to the FY19 DHS SBIR Phase I solicitation. This notice is not a solicitation or Request for Proposals. This notice is merely an opportunity for interested parties to comment on or request information about the attached topic areas.

THIS IS A PRE-SOLICITATION; IT IS NOT A REQUEST FOR PROPOSALS.

Pertinent information for the pending solicitation topic areas can be found in the attached **FY 19 SBIR Topic Areas** document.

The pre-solicitation period is from November 30, 2018 through December 18, 2018.

During the pre-solicitation period, technical questions concerning the topics should be directed towards the Technical Point of Contact (POC) for each topic, listed in **the FY 19 SBIR Topic Areas** document.

During this pre-solicitation period, interested parties have an opportunity to contact topic authors via email to ask technical questions about specific technical topics attached to this notice. Telephone inquiries will not be addressed.

Questions should be limited to specific information related to improving the understanding of a particular topic's requirements. **Potential offerors are prohibited from seeking advice or guidance on its solution approach, or submitting any materials**.

No further contact between offerors and Technical Points of Contact shall occur after 5pm EST on December 18, 2018.

The Government anticipates release of the final solicitation on or about December 19, 2018.

It is mandatory that potential offerors be registered on the following areas:

SBIR Portal (https://sbir2.st.dhs.gov)

U.S. Small Business Administration's (SBA) Company Registry Database (http://sbir.gov/registration)

System for Award Management (SAM) (www.SAM.gov).

Only small business, as defined in the Small Business Administration (SBA) SBIR Policy Directive, are eligible to respond.

7.0 Research Topics

7.1 S&T Directorate Topic

The following are the topics for the FY19.1 S&T Directorate's SBIR Program:

H-SB019.1-001 - Reach-Back Capability for Fielded Rapid DNA Systems
H-SB019.1-002 - ICAM On-the-Fly
H-SB019.1-003 - On Body Power Module for First Responders
H-SB019.1-004 – Modelling-based Design of Sensors for Chemical Detection in Complex Environment
H-SB019.1-005 - Synthetic Training Data for Explosive Detection Machine Learning Algorithms
H-SB019.1-006 - Cybersecurity Peer-to-Peer Knowledge/Lessons Learned Tool
H-SB019.1-007 - Network Modeling for Risk Assessment
H-SB019.1-008 - Blockchain Applications for Homeland Security Forensic Analytics

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

7.2 CWMD Office Topics

The following are the topics for the FY19.1 CWMD SBIR Program:

H-SB019.1-009 - Detector Integration with Current and Emerging Networked Systems
H-SB019.1-010 - Unmanned Aerial System Autonomous Search of Limited Area for Radiological Threats

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

APPENDIX A – RESEARCH TOPIC DESCRIPTIONS

SBIR TOPIC NUMBER: H-SB019.1-001

TITLE: Reach-Back Capability for Fielded Rapid DNA Systems

TECHNOLOGY AREAS: *Enhanced Border Security, Prevention of Human Trafficking and Smuggling, Multimodal Biometric Collection*

OBJECTIVE: Development of an accredited DHS reach-back capability to review results from fielded Rapid DNA systems using the Office of Biometric Identity Management (OBIM) DNA Store/Match/Share capability.

DESCRIPTION: The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) developed Rapid DNA technology under a prior Small Business Innovative Research (SBIR) program to provide family relationship verifications in the field, a capability that no other biometric provides. Rapid DNA is an innovative technology that reduces the testing and analysis time for Deoxyribonucleic Acid (DNA) from the classical three to six months down to 90 minutes using a printer-size portable device. Rapid DNA also internally analyses the DNA profiles and with OBIM Store/Match/Share software can verify family relationship claims of biological relatedness (kinship). This has direct application to improving processes and reducing fraud in immigration, human trafficking/ smuggling at the borders, and for reunification of families following a mass casualty event. This SBIR topic builds on the established Rapid DNA capability, adding the necessary capability to provide for reach-back review of Rapid DNA results in an accredited environment.

DHS S&T has had a significant role in developing, overseeing, testing and evaluating the Rapid DNA technology and it is now commercially available and ready to be implemented. Better than 90% of the time Rapid DNA produces a DNA profile cable of supporting a match and the instrument returns a green checkmark. But the remaining 8% of the time, the profiles receive either a yellow or red flag and need to be reviewed. Some of these yellow or red flags are due to issues with the DNA profile that will not impact the kinship analysis and some are due to processing issues by the technology. Either way, DHS needs an ability to reach-back to a DNA analyst to review the DNA profiles and to re-run a DNA sample when necessary. The DNA analyst and the facility also need to be accredited so that the fielded Rapid DNA results and those of the reach-back capability are shown to be repeatable and accurate to stand up in court, if challenged.

The DHS Customs and Border Protection (CBP) Laboratories and Scientific Services Directorate (LSSD) has multiple regional laboratories and satellite offices for the processing of multiple forensic sample types, but does not currently have a human DNA laboratory. We are seeking any innovative/alternative solutions that would provide a reach-back capability for fielded Rapid DNA systems, anticipating that the developed solution would ultimately transition into the LSSD laboratory for long-term operational support to DHS field components.

The research into potential reach-back solutions would need to address the analysis of innovative or potential solutions to provide reach-back support for Rapid DNA, the interface an analyst uses to review and annotate Rapid DNA field results, the use of DNA data sharing standards, the accreditation of the reach back capability, location/staffing/costs for the reach-back capability, and the eventual transition of the new capability to DHS LSSD facilities.

Once the alternative reach-back solutions are proposed, a pilot solution would be developed to implement the reach back capability. This would include specifying and acquiring the appropriate technology, developing the detailed documentation to establish and maintain accreditation, researching and developing training materials, establishing performance metrics and risk mitigation recommendations and measurement plans, and addressing access and privacy protection solutions.

PHASE I: The offeror shall research the feasibility of providing a reach-back solution for fielded Rapid DNA systems. A Phase I final technical report shall be submitted addressing the analysis of potential solutions to reach-back support for Rapid DNA, the use of DNA data sharing standards, the accreditation of the reach back facility or laboratory, facility location, staffing, costs, and the eventual transition of the new capability to DHS LSSD facilities.

PHASE II: Phase II continues the research that began in Phase I and develops a pilot solution to implement the reach back capability. This includes specifying and acquiring the appropriate technology for an analyst to review and annotate Rapid DNA results, developing the detailed documentation to establish and maintain laboratory or facility accreditation, researching and developing staff training materials, establishing performance metrics and risk mitigation recommendations and measurement plans, and addressing facility access and privacy protection solutions. Deliverables include monthly progress reports, a final technical report detailing the developed solutions, and a prototype reach-back capability that connects to at least one government provided Rapid DNA instrument.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: Phase III would transition the pilot solution into a DHS LSSD laboratory or other Government operational environment that would provide the ongoing operational reach-back for fielded Rapid DNA systems. All technical and operational policies and procedures would be established and validated and accreditation of the solution would be achieved. This will directly support DHS in the establishment of DNA as a biometric that supports family relationship testing for immigration, border patrol human trafficking/smuggling prevention and reunification of families following mass casualty events.

State and local law enforcement, medical examiners, and disaster preparedness agencies are all evaluating the use of Rapid DNA in their operations. This reach-back capability is necessary in all of those applications to ensure that their solutions are validated and accredited, and that a human analyst has the ability to review the results.

REFERENCES:

1. Rapid DNA Fact Sheet: https://www.dhs.gov/publication/rapid-dna
2. Rapid DNA Snapshot Article: https://www.dhs.gov/science-and-technology/news/2017/06/16/snapshot-rapid-dna-technology-makes-verifying-relationships
3. Rapid DNA News: https://www.dhs.gov/science-and-technology/rapid-dna

KEY WORDS:
Identity Management, Biometrics, DNA, Kinship, Accreditation, Reach-back Support

TECHNICAL POINT OF CONTACT: Christopher Miles, christopher.miles@hq.dhs.gov

SBIR TOPIC NUMBER: H-SB019.1-002

TITLE: ICAM On-the-Fly

TECHNOLOGY AREAS: *ICAM, Identity Proofing, Automatically Provisioning*

OBJECTIVE: Develop / demonstrate an Identity, Credential, & Access Management (ICAM) solution that will allow all first responders supporting a multi-jurisdictional event to be able to safely and securely share information.

DESCRIPTION: The Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) Project Responder 5 Report identified key capabilities to help first responders be more effective in their mission. Among the findings included the need to securely share information, validate responders from other organizations, and securely maintain records. These challenges only increase as responders rely on more data. There is a critical need for responders to securely validate users and share information. ICAM principles can mitigate these challenges.

ICAM is a framework of policies built into an organization's IT infrastructure that allows system owners to have assurance that the right person is accessing the right information at the right time for the right reason. First Responders need to safely and securely share information between jurisdictions, but first responder organizations do not currently have federations set up to aid in information sharing. Instead, during multi-jurisdictional responses, organization might be forced to manually provision an un-vetted new user or take days to vet a new user's identity and certificates. Lead agencies require quick and secure solutions to vet identities and credentials in real time as well as auto-provision users into information sharing applications. ICAM On-the-Fly would allow new users to show up to assist in a public safety event, bringing their own credential, their own device and the role they are to provide during the event.

Fundamentally, ICAM On-The-Fly must:

- Perform Quick Identity Proofing;
  (e.g. validate that the user is who they says they are)
- Validate applicable certifications and attributes required to access the information to be shared; (e.g. EMT Certified, sworn law enforcement)
- Automatically Provision (register) New Users;
- Be built using open standards to preserve interoperability;
- Be cross platform (iOS/Android) compatible; and
- Recognize a broad array of credential attributes in diverse environments (i.e. multiple types of LDAP, Active Directory, etc.)

PHASE I: During this phase, the SBIR performer will conduct a technical analysis and propose a development road map for constructing an ICAM On-The-Fly solution. The technical analysis will identify the state-of-the-art identity proofing, application validation and automatic provisioning technologies using its own or industry R&D resources. This technical analysis must identify the technical gaps that the performer will incorporate as part of its proposed solution architecture. At a minimum, the performer shall cover the following:

- Identification of Public Safety stakeholder requirements
- Evaluation of current services, tools and commercial capabilities
- Determination of open standards and connectors to enable interoperability to maintain compatibility with NIST SP 800-63-3

The development roadmap to construct an ICAM On-The-Fly system must show the steps necessary to produce a minimum viable product (MVP) including at a minimum:

- A system architecture, inclusive of multifactor authentication using open standards such as FIDO U2F and NIST SP 800-63A (built to at least, IAL2: remote proofing);
- A complete set of system policies, including but not limited to, credential attestations to be harmonized across entities, and aggregate and weighted values for credentials being vetted from multiple truth sources; and
- A development work plan clearly demonstrating the path to completion.

PHASE II: Phase II continues the research that began in Phase I and will deliver a prototype implementation designed to meet the ICAM On-The-Fly needs. The prototype will be demonstrated in test and evaluation in an operational exercise to demonstrate the capability. At a minimum, Phase II should include the following:

- A MVP;
- Build proof of concepts to integrate commercially available products with the MVP;
- Simulate and demonstrate an operational environment;
- Document implementation guides, lessons learned, and custom code.

The final technical report detailing the technical analysis and proposed solution architecture.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: Phase III may include further technical development to address gaps discovered during the test and evaluation and further end-user feedbacks. The research and development efforts from Phase III will results in the commercial or government application in which at least one agency will take delivery of the tool and its services. Example may include:

- Delivery of the automated tool via network-as-a-service or software-as-a-service to a designated public safety agency for end-user application
- Standalone tool delivered to designated commercial or public safety agency with standard tool training and technical support

REFERENCES:

1. FIDO U2F - https://fidoalliance.org/download/
2. NIST SP 800-63 - https://pages.nist.gov/800-63-3/
3. NIST SP 800-63A - https://pages.nist.gov/800-63-3/sp800-63a.html
4. NIST SP 800-63-3 - https://pages.nist.gov/800-63-3/sp800-63-3.html
5. NIST SP 800-53 - https://nvd.nist.gov/800-53

KEY WORDS:

Identity, Credentials, Access Management, Multifactor Authentication, Federation, Cyber Security, Information Sharing

TECHNICAL POINT OF CONTACT:

Norman Speicher, norman.k.speicher@hq.dhs.gov

SBIR TOPIC NUMBER: H-SB019.1-003

TITLE: On Body Power Module for First Responders

TECHNOLOGY AREAS: *Communications, Sensors, Internet Of Things (IoT), Power Systems, Batteries, Rechargeable*

OBJECTIVE: Develop a module that can power/charge and provide effective power management of all on-body electronics including sensors, communications systems, and peripheral devices for all first responder mission areas including: EMS, fire and law enforcement.

DESCRIPTION: First responders will need to carry many more devices such as sensors (environmental, physiological monitoring, hazard), IoT devices in addition to their cell phones and radios and peripheral devices (e.g., heads up displays) that require power. Each of these devices may have different power requirement (e.g., USB, USB-C, Apple, microUSB) and may need to be charged at different intervals depending on battery life and use. Requiring first responders to charge and track battery levels for all these devices would be an additional burden and work load. The innovation sought here is to develop a power module for first responders (PMFR) that would service all the current and emerging requirements of on-body devices. The Power Module would provide long-term, exchangeable and rechargeable battery power to the various modules for extended use.

Currently, DHS is aware of some power modules/battery pack that have been developed for Department of Defense (DoD) applications but none for the first responder civilian applications. It is anticipated that in the future if these power modules are deployed ubiquitously then sensors and peripheral devices no longer need built-in power systems and can rely on the PMFR for power. Use of external power subsystems would then reduce the costs, size and form factor of sensors and peripheral devices.

The PMFR should be:

- Flexible to support a number of devices and power requirements (IoT devices, sensor modules, cellular and radio systems)
- Swappable (swap out a unit with a low charge with a fully charged device); ideally hot swappable
- Portable (low size and weight for use on day to day applications and for carrying)
- Low cost (objective $50/threshold $100 for non-intrinsic models)
- Available for different applications (intrinsically safe for fire applications or standard ruggedized for EMS or law enforcement IP68 or CSA for intrinsic applications)
- Operate for 24 hours (objective) or 8-12 hours (threshold))
- Rechargeable through 110 Volts or 12 volts (from vehicle)
- Capable of providing battery status, report run-time remaining and alert when charge falls below a threshold
- Capable of using standard battery or batteries (for backup)
- Capable of detecting and reporting modules connected to the Power Module and provide battery status

- Power status application with low-power alert function;

PHASE I: Phase I will have the following outputs:

- Determine current and future power requirements for first responder applications by assessing what equipment may be connected and power requirements
- Develop an architecture that uses as reference the Next Generation First Responder handbook
- Develop a design and proof of concept including defining size (dimensions and weight) and form factor; design should account for minimal impact to user profile
- Propose battery type and safety considerations
- Define packaging and specifications for both the intrinsically safe and standard configuration (IP68, CSA 157)
- Develop a cost model to determine the approximate costs of each of the two types (intrinsically safe and standard); cost model should also define required volume discounts

PHASE II: Develop a minimum of 10 standard and 5 intrinsically safe (CSA) power modules. During Phase II, detailed testing shall be conducted to assess and demonstrate performance of the unit both in a laboratory environment and field demonstration to assess form fit function. Detailed test report on charge/discharge cycles along with battery life should be documented. Final report should include an evaluation of the prototypes against all the requirements documented above and in Phase I.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: Applications of this product and prototypes should provide the capability of low cost power module for use by all first responders (federal, state and local). This product could also expand and be used for DoD applications as well.

REFERENCES:

1. NGFR Integration Handbook version 3.0 developed by DHS S&T; https://www.dhs.gov/publication/st-frg-ngfr-integration-handbook-version-20;
2. Smart battery definition, http://smartbattery.org/specs/sbdat110.pdf
3. CSA C22.2 NO 157 Intrinsically safe and non-incendive equipment or use in hazardous locations

KEY WORDS:

Power Systems, Batteries, Rechargeable, portable power

TECHNICAL POINT OF CONTACT:

Sridhar Kowdley, Sridhar.kowdley@hq.dhs.gov

SBIR TOPIC NUMBER: H-SB019.1-004

TITLE: Modeling-based Design of Sensors for Chemical Detection in Complex Environment

TECHNOLOGY AREAS: chemical detection, chemical sensors, molecular-based modeling, Monte Carlo

OBJECTIVE: Develop sensors for chemical analyte detection based on existing theoretical models and compare their selectivity and sensitivity characteristics with the model predictions.

DESCRIPTION: DHS and first responders need low cost, high performance sensors that can be used to detect chemical materials in different environments. A persistent problem in chemical sensing is the inability of the sensor system to reliably address complex sensing tasks and environments. Such conditions are regularly encountered in situations involving environmental monitoring, industrial process control, toxic chemical and fire detection. Often, these tasks are centered on the detection of chemical signatures rather than individual chemical compounds. However, detection of individual analytes is often complicated significantly by environmental conditions that exist in backgrounds with multiple potentially interfering chemical species. This can lead to surprisingly poor performance in real-world environments after excellent results have been demonstrated in the laboratory. Hence understanding the surrounding details of a chemical sensing problem is critical to finding a solution, together with knowing and addressing the target analytes themselves.

Different types of sensors, a large number of them being based on molecular sensing capability and coupled with nanostructured surfaces, are being developed. However, most of these sensor developments are empirical and their performance, particularly the interplay between sensitivity and selectivity, cannot be predicted until the sensors are fully tested in a real-world environment. The costs to the user are therefore quite substantial for each sensor development before an objective assessment with regards to their usability can be made. On the other hand, a modeling-based approach, which would allow design of surfaces as well as the sensing device diagnostics, could allow for an inexpensive, user friendly approach to designing sensor materials that can be integrated with electronics to produce any type of sensor – chemical or biological, with parts per trillion (ppt) sensitivity and fast (seconds) response times. The reduction in cost compared to the current sensor development approaches which are empirical in design is expected to be at least an order of magnitude.

Many current sensor developments involve different types of polymers like those used in surface acoustic wave (SAW) mode or molecular imprinted polymer (MIP) configurations. A recurring problem with regards to sensing of chemical vapors is the issue of addressing complex sensing tasks and environments that are routinely encountered in most real-world situations. Even detection of individual analytes is almost always complicated significantly by these unavoidable environmental conditions. This can lead to surprisingly poor performance in environments relevant to first responders [1,2]. The same selectivity problem exists even in the case of arrays of sensors [1]. Theoretically based strategies for design and optimization of chemical sensors are rarely adopted by sensor developers. The same situation also exists for molecularly imprinted polymers. Molecular imprinting is the process whereby a polymer matrix is cross-linked in the

presence of molecules with surface sites that can bind selectively to certain ligands on the polymer. Recent theoretical work [3,4] has discussed a model that accounts for the key features of this molecular recognition approach. Using a combination of analytical calculations and Monte Carlo simulations, it has been shown that the model can account for the binding of rigid particles to an imprinted polymer matrix with valence-limited interactions. It has also been shown as to how the binding multivalency and the polymer material properties affect the efficiency and selectivity of molecular imprinting. These calculations also indicate pathways to formulate design criteria for optimal molecular imprinting. While theoretical models for rational design of sensors and sensors arrays do exist, there has not been any sensor development which is explicitly based on these models. The goal of the project is to develop sensors based on the rational designs of the theoretical models and evaluate the sensor performance in both pristine and complex environments relevant to the needs of the user community.

PHASE I: The Offeror shall design and develop one type of sensor based on the rational design of the sensor based on any one of the existing theoretical models [1-4]. The Offeror shall demonstrate that the sensor can have high selectivity (better than 0.1 parts per billion) for the detection of chemical vapors of a chemical agent simulant or a toxic industrial chemical in the vapor phase. The Offeror shall demonstrate that the sensitivity is not compromised by the simultaneous presence of three different types of interfering gas molecules. The interfering gases should possess chemical, physical or spectral properties similar to the target chemical vapor. The matrix for success will be a demonstration of less than a factor of 10 reduction of sensitivity for the detection of the target chemical vapor in presence of the contaminant gases.

PHASE II: The primary prototype to be developed in this project is the computational model that can be used in future sensor development efforts. The Offeror must demonstrate the capability of the model by fabricating 8x8 sensor arrays with integrated measuring electronics. The Offeror shall compare the sensor array response performance in terms of the response to different analytes and different contaminant gases, specific identifies of which will be selected during Phase I. The Offeror shall assess the sensitivity benefit when combining two or more sensors with the same sensitivity. The goal of Phase II is to show that the sensor array is capable of detecting different types of chemical analytes with the same sensitivity in the simultaneous presence of different types of contaminant molecules. Ten (10) prototype 8x8 sensor arrays shall be produced. A major goal of the Phase II is to prove that by using the selected model, future sensor design processes will be more efficient and reduce development time and costs.

In addition to the field testable prototype, deliverables include; a quad chart (template will be provided), a one pager (template will be provided), and monthly status calls. A commercialization plan must be completed, identifying specific customers, completed outreach to those customers, licensing requirements, pricing and future upgrades.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: The results of this effort would establish a computational method to more efficiently design sensor materials significantly impacting the time and cost to development and commercialization of sensors for both chemical and biological environmental contaminants. First responders have a need for detection systems for situational awareness as well as several DHS components (e.g., Customs and Borders Protection, United States Coast Guard) used during daily operations.

REFERENCES:

1. Kevin Johnson and Adam Knapp, "Selectivity Measure for Arrays of Non-Specific Sensors", Sensors and Actuators B 251, 1076-1088 (2017).
2. Kevin Johnson and Susan L. Rose-Pehrsson, "Sensor Array Design for Complex Sensing Tasks", Ann. Rev. Anal. Chem. 8:14.1-14.24 (2015).
3. Tine Curk, Jure Dobnikar and Daan Frenkel, "Rational Design of Molecularly Imprinted Polymers", Soft Matter, 12, 35-44 (2016).
4. Dumitru Pavel, Jolanta Lagowski and Carmela Jackson Lepage, "Computationally Designed Monomers for Molecular Imprinting of Chemical Warfare Agents – Part V", Polymer 47, 8389-8399 (2006).
5. Braden C. Giordano and Greg E. Collins, "Synthetic Methods Applied to the Detection of Chemical Warfare Nerve Agents", Current Organic Chemistry, 11, 255-265 (2007).

KEY WORDS:

Chemical Sensor, Rational design of sensor, Model based sensor design, Sensors for complex environment, Molecular Imprinting of Polymer, Surface Acoustic Wave Sensor

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

SBIR TOPIC NUMBER: H-SB019.1-005

TITLE: Synthetic Training Data for Explosive Detection Machine Learning Algorithms

TECHNOLOGY AREAS: Millimeter-Wave (MMW) and X-Ray explosive detection systems, passenger checkpoint, checked baggage

OBJECTIVE: Development of methods for creating synthetic human subject/baggage object models for creating realistic image-based machine learning training data

DESCRIPTION: Currently fielded explosive detection equipment uses electromagnetic signals, such as X-rays or MMWs to interrogate passengers and their belongings. Automatic algorithms process the images generated by the screening hardware either to clear the passenger/property or to identify specific anomalies for further investigation. The use of machine learning and deep learning approaches to develop these algorithms have shown significant promise in improving overall system performance. The DHS S&T/TSA Passenger Screening Algorithm results showed the effectiveness of deep learning applied to passenger screening. Development of the equipment and its associated detection algorithms is time consuming and expensive because system screening performance is difficult to accurately model. Currently:

- Prototype systems must be built and tested to measure and understand the interaction of X-rays/MMWs with explosives in various containment configurations.
- Development requires physical test articles to be fabricated or acquired. Suitable test articles may be impossible to create if the explosives involved are unsafe to synthesize.
- If machine learning or deep learning algorithms are developed for detection, many test articles must be created and scanned to build datasets for algorithm development, training, and testing. This is particularly labor intensive in order to generate large, representative datasets.

In order to accelerate the advancement of explosive detection equipment, the DHS S&T Directorate seeks to develop tools to create virtual models of human travelers, their baggage and its contents. These models:

- Should be representative of the stream of commerce.
- Should be capable of including simulated explosives and prohibited items.
- Should be able to be generated in large numbers (many thousands or millions) in a reasonable amount of time (under 1 second per image).
- Should be useable by researchers and vendors to predict the performance of emerging explosive detection technologies and to train machine learning-based detection algorithms. The predictions and training will make use of tools (see, for example, https://www1.aps.anl.gov/science/scientific-software) that simulate the propagation of X-rays/MMWs through simulated objects.
- Should be useable for assessing a system's ability to detect emerging threats that are unsafe to synthesize.
- Should be useable for a variety of electromagnetic interrogation methods including synthetic aperture radar, computed tomography, and single and multi-view (AT2) line scanners. These technologies use transmission, diffraction, and phase contrast to detect explosives and prohibited items.

The tools should:

- Include methods to create shape descriptions for explosives and other objects, and methods to insert these items into representative scans. The mathematical descriptions may be based on the union of geometric primitives, polygon meshes, and sampled three-dimensional volumes.
- Include parametric descriptions for the features of explosives, so that users do not require access to classified information.
- Be compatible with tools in the public domain for simulating X-ray/MMW interactions with objects.
- Be compatible with script- or code-based algorithms targeting open-source multi-dimensional modeling software (*e.g.*, MakeHuman and Blender)
- Provide for a real-time means of dynamic configurability, especially as regards the physical properties of virtual materials to be used in the modeling and the system's input/output file pathways (*e.g.*, use of "config files")

PHASE I: Applicable publicly and commercially available tools for X-ray and electromagnetic simulation as well as for generating stream of commerce objects shall be evaluated. Initial simulations shall be performed combining selective tools with additional algorithms to determine whether data representative of existing human subject, bags and cargo containers can be created. Build a small number of simulated passengers and bags. Write a project plan, including system requirements, technical approach, estimated costs and schedule, for Phase II. The deliverables include technical reports reviewing available tools and describing how existing passengers and bags are matched and a project plan for Phase II.

PHASE II: Develop software to simulate human subjects and checked baggage with all appropriate ancillaries (clothing, shoes, hair and, in the case of baggage, typical contents). Create at least 200 human subjects and 200 bags meeting the 1 second per image requirement. Deliverables include prototype software for the simulation programs, technical reports describing how the tools operate and how they were validated, and mathematical descriptions of the simulated human subjects, bags (and contents) and cargo containers, and scripts for generating the models of human subjects, ancillaries (clothing, shoes, hair, *etc…*), virtual baggage and contents.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: The tools could be sold commercially for use by screening equipment vendors. The provider could sell services to help vendors use the tools. There will be on-going expenses to modify the tools based on user feedback. DHS could supply the tools, or test sets of simulated baggage created using the tools, to vendors as part of future programs.

REFERENCES:

1. Schmidt, *Tools For Simulating CT Scanners*, in *Algorithm Development for Security Applications, Eighth Workshop (ADSA08), Automated Threat Recognition (ATR) Algorithms for Explosion Detection Systems*, Northeastern University, Boston, October 24-25, 2012, http://myfiles.neu.edu/groups/ALERT/strategic_studies/ALERT_ADSA08_final_report.pdf

2. *FORBILD phantoms (standard for medical CT)*. http://www.imp.uni-erlangen.de/phantoms/
3. *Geant4 - a toolkit for the simulation of the passage of particles through matter*, http://geant4.cern.ch/
4. Kak and Slaney, *Principles of Computerized Tomography*, IEEE Press, released into the public domain at: http://www.slaney.org/pct/
5. DHS S&T/TSA Passenger Screening Algorithm Challenge: http://www.kaggle.com/c/passenger-screening-algorithm-challenge/

KEY WORDS:
x-ray, millimeter-wave, simulation, computerized tomography, diffraction, synthetic data

TECHNICAL POINT OF CONTACT: Karl Harris, karl.harris@hq.dhs.gov

SBIR TOPIC NUMBER: H-SB019.1-006

TITLE: Cybersecurity Peer-to-Peer Knowledge/Lessons Learned Tool

TECHNOLOGY AREAS: Cybersecurity, Information Sharing, Risk Analysis

OBJECTIVE: Develop a collaboration tool for medium/small organizations to help them identify key cybersecurity information and lessons-learned of most significance to them.

DESCRIPTION: Organizations throughout the American economy and government are faced with designing and then operating cybersecurity risk management, in a complicated and dynamic environment. They have been provided with a useful starting point, a cybersecurity risk management framework, developed by NIST, supported by DHS, and filled out in some detail by different critical infrastructure sectors and organizations. But sustaining risk management operations is more difficult, as organizations must somehow blend a great deal of technical input (vulnerability reports, incident reports, threat analysis, technical guidance, etc.) with their own organizational experience. The cybersecurity "knowledge management" challenge is significant for any particular organization, regardless of size or critical infrastructure domain.

Additionally, several million organizations and companies across the country are faced with this challenge, continuously. Most information sharing systems assume that these many organizations and companies should report their cybersecurity experiences vertically to commercial and governmental centers, which are to synthesize these various reports and report back analytical insight. But what does not yet exist is a peer-to-peer version of this reporting activity, where an organization can directly leverage related experiences of thousands of organizations and companies, through a tool that can capture and report their own experiences and connect them with comparable experience of other organizations and companies, to better help them understand and manage their cybersecurity risk.

The end product of this effort should address capabilities such as:

- Key internal risk assessment elements
- The time/dynamics of internal risk assessment elements
- Outside context for these assessments (vulnerabilities, operating data, etc.)
- Multiple information sharing mechanisms (one to one, one to many, collaboration drafts, etc.)

The key requirement is that this tool must be able to support enterprise consideration of cybersecurity risk, by bringing into the process valuable insight from other enterprise' consideration of risk

PHASE I: The expected focus of the Phase I effort is to assess (A) relevant knowledge management practices and capabilities, and (B) peer-to-peer information sharing principles, systems and experiences, both with respect to the cybersecurity information sources and the technical and operating environment. The Phase I effort must develop a tool design and architecture, a technical CONOPS for how the tool would be used in realistic business environments, and a development strategy that involves substantial operational participation, i.e. how would Phase II be conducted in partnership with real companies and organizations and their

operational environments. Phase I deliverables must include a final technical report addressing tool design/architecture, expected CONOPS and the proposed development strategy, and a presentation addressing this need and work.

PHASE II: The Phase II effort will develop the prototype peer-to-peer information sharing tool, demonstrate/pilot the use of this tool for 60-90 days by at least five small to medium sized organizations or companies, and revise the tool design and architecture reflecting the Phase II experience. Phase II deliverables will include a prototype tool, a final technical report that includes both a revised tool design/architecture and the initial operating experience of the five (or more) small to medium sized organizations, and a revised presentation addressing this need and work.

PHASE III (COMMERCIAL OR GOVERNMENT APPLICATIONS): Phase III will include several different activities, all of which are intended to expand awareness, development and application of this capability, via sustained user engagement.

- ❖ Further development of the tool (both technical elements and operational experience), and placing this tool out on GitHub for open use.
- ❖ Application of this tool to several different critical infrastructure sectors, via Information Sharing & Analysis Centers/Organizations.
- ❖ Application of this tool to several different government organizational environments, such as the Federal CISO Council.
- ❖ "Uptake" of this tool into existing commercial cybersecurity capabilities operating in the market now.

REFERENCES:

1. https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity
2. https://www.cisecurity.org/ms-isac/ms-isac-toolkit/
3. https://its.ny.gov/eiso/local-government
4. https://bc2m2.pnnl.gov/
5. https://www.cooperative.com/remagazine/articles/Pages/Cybersecurity-Research-at-NRECA.aspx
6. http://130.18.86.27/faculty/warkentin/BIS9613papers/Baskerville1991_EJIS_1_2_risk_analysis.pdf
7. https://www.hsdl.org/?view&did=808477\

KEY WORDS:

Cybersecurity, Information Sharing, Peer-to-Peer, Expert System, Risk Assessment, Lessons Learned.

TECHNICAL POINT OF CONTACT: Dr. Christos Papadopoulos, christos.papadopoulos@hq.dhs.gov

SBIR TOPIC NUMBER: H-SB019.1-007

TITLE: Network Modeling for Risk Assessment

TECHNOLOGY AREAS: modeling of systems, risk assessment, counterfactual analysis

OBJECTIVE: Develop models of networks to identify risks associated with the network, tool development for counterfactual analysis (what-if scenarios), and risk assessment

DESCRIPTION Networks, and systems of networks are ubiquitous in modern technology used throughout society today. Identification of risk in these networks often requires a model to be developed for the network or system of networks. These models range from the simple to the mathematically complicated models used for large networks. Some risks, such as cascading failures in a network, are difficult to identify. The goal for this effort is to develop the tools necessary to identify these risks, with a potential to identify mitigation strategies with an initial focus on emergency communications networks.

The tool should be capable of including information about the network, such as number and type of nodes, appropriate labels for nodes, and known risks or defects for the network. The tools will also be capable of performing counterfactual or "what-if" analysis, to identify risks in the network, such as the potential for cascading failures. The tool shall be able to incorporate information about the network or system from the PARIDINE project. PARIDINE is intended to provide disruptive event information for large networks or the Internet. This includes: 1) a definition of a disruptive event; 2) identification of data to identify disruptive events; 3) identification and operational reporting via an API for disruptive events and 4) attribution or root cause analysis of the disruptive events, with a measure of attribution accuracy. At least three state space models will be produced under the phase I effort.

PHASE I: The final deliverable for Phase I proposals is an initial proof of concept design for a risk assessment tool that incorporates state space models of networks or systems of networks. At least one state space network model shall be of a large network, the size of a multinational corporation network or government agency network. All models will include modeling of privacy in the network. At least one model shall be of an emergency communications network, or part of an emergency communications network. Examples include call flow within a 9-1-1 system of various sizes (e.g. small, less than 5 seats). The proof of concept design shall include algorithms to identify risks in the state space models produced under the phase I effort.

PHASE II: The deliverable for Phase II is a prototype software or device/software combination that implements the proof of concept design in Phase I. The prototype should be applicable to government and enterprise communication networks or systems of networks, and ideally include mobile devices. The developed prototype will be delivered for piloting, within DHS components, other government organizations, or enterprises. Additional state-space system or network models may be required for the pilot implementation. The risk assessment tool will include analysis for privacy risks in the network.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: Although the focus of this effort is for emergency communications networks, and call flow within 9-1-1 systems in particular, the tool(s) developed under this project will have many applications in both industry and government. Enterprise networks are compromised on a regular basis. Identification of risks associated with government and enterprise networks will benefit the entire internet ecosystem to enable protection and mitigation activities.

REFERENCES:

1. 9-1-1: https://www.911.gov/pdf/OEC_NG911_Cybersecurity_Primer_May_2018.pdf
2. 5 Steps to Perform a Cyber Security Risk Assessment on Your Network https://peoplesec.org/2018/02/25/5-steps-perform-cyber-security-risk-assessment-network/
3. NIST risk assessment framework: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

KEY WORDS:

Network Modeling, Cyber Risk Assessment, Counterfactual Analysis, Network Risk Assessment, Privacy risk, 9-1-1 cyber risk

TECHNICAL POINT OF CONTACT:

Ann Cox, Ann.Cox@hq.dhs.gov

TOPIC NUMBER: H-SB019.1-008

TITLE: Blockchain Applications for Homeland Security Forensic Analytics

TECHNOLOGY AREAS: Encryption, authentication, cyber security, internet of things, and data analytics, blockchain

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

DESCRIPTION: Blockchain and Distributed Ledger Technology (DLT) are emerging technologies being leveraged for a wide range of commercial and governmental applications. The most well-known use case would likely be Bitcoin, within the newly emerged cryptocurrency arena, which has spurred further interest and developments. Prior efforts have addressed Bitcoin analytics, which covers only a limited scope within the realm of cryptocurrencies. This proposal seeks applications of blockchain forensic analytics for newer cryptocurrencies, such as Zcash and Monero. And, ongoing research within the field also contributes to new technological implementations and techniques that continue to multiply the specific types of consensus, privacy, security, and proof mechanisms.

A key feature underlying these newer blockchain platforms that is frequently emphasized is the capability for anonymity and privacy protection. While these features are desirable, there is similarly a compelling interest in tracing and understanding transactions and actions on the blockchain of an illegal nature. To that end, this proposal calls for solutions that enable law enforcement investigations to perform forensic analysis on blockchain transactions. This analysis can be approached in any number of ways and may consider different data situation use cases depending on whether additional data from off-chain sources are available. Furthermore, with the proliferation of new blockchain variants, the desired solution should either attempt to show generality or extensibility, or at least provide working approaches to treating newer blockchain implementations.

PHASE I: Design a blockchain analysis ecosystem or modify an existing one, that enables forensic analysis for homeland security and law enforcement applications for cryptocurrencies, such as Zcash and Monero. Produce an architecture that shows how system components can be upgraded or interchanged for an extensible and forward-looking solution that can be maintained for use with emerging blockchain networks. 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 and demonstrate the blockchain forensic technologies designed during Phase I. The demonstrations will include three (3) use cases determined by DHS/S&T and will involve the analysis of suspicious transaction without external data, with external data, and on another blockchain platform. A technical report detailing the results and improvements made to enhance the technology will be provided after each demonstration.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: The proliferation of blockchain technology beyond the cryptocurrency arena has drawn interest from all other sectors, with new proposed blockchains for everything from banking, charitable donations, supply chain tracking, to automatically executing "smart contracts". These technologies stand to radically transform operations in government and the private sector. 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. Blockchain forensic analytics for the homeland security enterprise can help the DHS law enforcement and security operations across components as well as state and local law enforcement operations. Private financial institutions can likewise benefit from such capabilities in enforcing "know your customer" and anti-money laundering compliance.

REFERENCES:

1. https://www.technologyreview.com/s/610807/sitting-with-the-cyber-sleuths-who-track-cryptocurrency-criminals/
2. https://coincenter.org/entry/how-can-law-enforcement-leverage-the-blockchain-in-investigations
3. https://cointelegraph.com/news/how-law-enforcement-can-investigate-bitcoin-related-crimes-and-why-thats-good
4. https://www.inc.com/will-yakowicz/startups-law-enforcement-agencies-catch-criminals-who-use-cryptocurrency.html
5. https://www.bloomberg.com/news/articles/2018-06-27/fbi-has-130-cryptocurrency-related-investigations-agent-says

KEY WORDS:

Encryption, crypto-certification, encrypted data analytics, authentication, cyber security, internet of things, blockchain, and data analytics

TECHNICAL POINT OF CONTACT: Stephen Dennis, Stephen.Dennis@hq.dhs.gov

SBIR TOPIC NUMBER: H-SB019.1-009

TITLE: Detector Integration with Current and Emerging Networked Systems

TECHNOLOGY AREAS: Data Communication Networks, Cloud Computing, Radiation Sensing, Internet of Sensors.

OBJECTIVE: Survey current radiation instruments/sensors used for preventative radiological/nuclear (R/N) detection missions. For selected systems, develop appropriate interfaces that permit integration with current and emerging networked systems.

DESCRIPTION: This topic seeks the development of relevant communications protocols, application programming interfaces (APIs), and interface control documentation (ICDs) to allow legacy and emerging radiation detection systems in operational use to be integrated into current and emerging networked systems. The effort would encompass surveying commonly deployed legacy radiation detection systems, cost-benefit analyses to assess the relative importance of which detection systems merit integration, and subsequent development of the required interfaces to permit integration of those systems.

The effort must include the ability to transmit/stream the data from the sensor(s) to current and emerging networked systems. It should take into account that there are a multitude of sensors that can be categorized as permanent, deployable, and roving, all of which can be in GPS-denied environments. Proposed technical solutions must provide near-real-time transmission of sensor data when cellular or WiFi communication is unavailable. These capabilities are critical to operational environments where cellular is not readily available, such as U.S. Coast Guard operations, and U.S. Customs and Border Protection (CBP) U.S. Border Patrol (BP) operations. Solutions should be proposed that are capable of high bandwidth, secured, rugged, scalable, cost effective, and low size, weight, and power. Additionally, solutions that allow transmission of data while minimizing signatures for geolocation of the transmitter would also permit a wider range of CONOPS.

Proposers should expect to develop working relationships with original equipment manufacturers (OEMs) of deployed legacy R/N detection systems and current performers supporting the current networked system.

PHASE I: Phase I efforts should lead to an initial demonstration of the detection system communicating with a current or emerging network and displaying appropriate responses to detected radiation source. This includes the following:

- Conduct a survey of deployed legacy radiation detection systems, and potentially other radiation sensors in addition to a preliminary cost-benefit analyses to assess the relative important of which detection systems merit integration. The following criteria must be factored into the cost-benefit analysis, along with any supplemental proposed criteria:
    - Prevalence of use of the legacy system
    - Cost of the system.
    - Performance of the system as compared to existing systems.

    - Existing communications capabilities of the system.
- Down-select a sample of these detection systems that are prioritized to integration with current networked systems.
- Develop and document required ICDs and/or APIs to support integration of the highest priority detection system.

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

PHASE II: This phase will expand upon Phase I, conducting the actual research and development to integrate three or more detection systems into the emerging network edge. This phase will conclude in demonstrated integration of several detection systems into the emerging network framework. This demonstration will include:

- Continuous, reliable communications of the instruments with current and emerging networked systems over an extended period of time (weeks).
- Effective ingestion and, as appropriate, analysis of detector data by the receiving network, including sensor state of health

Phase II deliverables include monthly progress reports and annual technical reports. Summary reports on three or more detection systems being successfully integrated on current and emerging networked systems are also required. Project review meetings will be held throughout the project period as needed to include but not limited to the initiation, mid-point and completion of the Phase II effort.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: This topic's Phase III activities would include a successful commercialization strategy for supporting the integration of other detection systems into the current/emerging network system and supporting their optimal use within the network.

REFERENCES:

1. Android Windows Tactical Assault Kit (https://atakmap.com/)
2. ArcGIS (http://www.arcgis.com/index.html)
3. Defense Advanced Research Projects Agency (DARPA) SIGMA project (See: https://www.darpa.mil/program/sigma; https://www.darpa.mil/news-events/2017-03-01; https://www.darpa.mil/news-events/2016-10-11; https://www.darpa.mil/news-events/2016-08-23

KEY WORDS: Data Communication Networks, Cloud Computing, Radiation Sensing, Internet of Things.

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

SBIR TOPIC NUMBER: H-SB019.1-010

TITLE: Unmanned Aerial System Autonomous Search of Limited Area for Radiological Threats

TECHNOLOGY AREAS: radiation detection, cost effective equipment, autonomous robotics, unmanned aerial system, UAS, unmanned aerial vehicle, UAV

OBJECTIVE: Integrate commercially-available radiation detection equipment into a commercially-available Unmanned Aerial System (UAS) to meet the objective of performing an automated search of a defined limited area (Cargo Container Yard, Stadium, Parking Lot, etc.) for radiological threats.

DESCRIPTION: The goal of this effort is to prove the concept of automated UAS to conduct radiation detection operations in a cluttered three-dimensional environment such as a cargo container yard, stadium, or parking lot. The only operator action will be to define the boundaries of the environment to be searched, to include defining basic search parameters (e.g. minimum separation distance from obstacles and flight line spacing). The UAS may include multiple small unmanned aerial vehicles. UAS capabilities must include:

1. Operation within 2 m of objects to be inspected during flight.
2. Detection of anomalous gamma-ray and neutron radiation. The onboard radiation detection systems will meet the radiological test detection requirements of the ANSI N42.48.
3. Production of a real-time “heat map” for radiation as flight is conducted.
4. Dwelling at locations where radiation anomalies are identified for as little as 30 seconds and no more than 5 minutes.
5. Optimization of search pattern to minimize search time while maintaining the ability to localize and identify radiological threats, including the ability to provide the operator with search time and battery usage estimates based on the definition of optimized search area and flight parameters provided by the operator.
6. LIDAR for collision avoidance and to map search area and using that information to develop an optimized search pattern.
7. Visual cameras to provide live feed of flight profile.
8. The ability to transmit location information of one small unmanned aerial vehicle (UAV) relative to the object being scanned and other unmanned aerial vehicles (if applicable).
9. Logging and transmitting to the operator and/or a designated reachback center geo-referenced gamma-ray spectra, visual imagery, LIDAR profile, and all flight parameters when the UAS records either a gamma-ray or neutron alarm.
10. Flexible communications (Satellite, Cellular Tower, Wireless, hardwired, etc.) depending on what is available at a given deployment location.

11. The ability to launch from a designated site, perform search, and return before running out of power or when "mission" is complete.
12. Communication of system health status back to operator ("heartbeat").
13. Recharging for subsequent assignment.
14. A human interface that allows for all automated functions to be controlled manually.
15. A "kill" button for emergency power-down on both the human interface and the unmanned aerial vehicle itself.
16. Field repairs on limited life components prone to deteriorate due to the nature of their function/design.
17. Running full diagnostics on the UAS platform for maintenance purposes as well as firmware updates, etc.

PHASE I: The end product of the Phase I effort should be a conceptual design for a UAS autonomous search system capable of detecting radiological threats in a complex 3-D environment such as a cargo container yard, stadium, or parking lot. The system should be capable autonomous operations in a cluttered 3-D environment. The design should identify commercial components that can be procured in Phase II and the design of the control component of the integrated system that will orchestrate the operation of the UAS vehicle and radiation detection system to carry out the screening. A simulation of the automated system is desired but not required. Other Phase I deliverables will be monthly progress reports and a final conceptual design report.

Phase I proposals should identify threshold and objective parameters for system cost, inspection time in clear weather, inspection time in "inclement" (as defined by the proposal) weather, detection distances and activity, system size and weight, system operation time, as well as any other performance parameters which are key to the specific UAV chosen. Proposals should emphasize integration of systems and components which are already commercially available, and should not contain significant R&D of UAVs or radiation detection systems.

Project review meetings will be held at the initiation, mid-point and completion of the Phase I effort.

PHASE II:
The end product of the Phase II effort should be the demonstration of UAS autonomous search system capable of detecting radiological threats in a complex 3-D environment such as a cargo container yard, stadium, or parking lot. After designating the optimized search area and flight parameters provided by the operator, the UAS prototype should carry out the screening, including transmission of the findings and spectra to a designated reachback center without further human intervention.

Phase II deliverables include monthly progress reports and annual technical reports. Two prototype systems will be delivered to CWMD (or its partners, as directed) at the end of Phase II. (This deliverable may be reduced or waived, depending on anticipated system cost.) Project

review meetings will be held throughout the project period as needed to include but not limited to the initiation, mid-point and completion of the Phase II effort.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS:
Should the concept be proven successful for a complex 3-D environment, the system could be modified to explore other Homeland Security applications, to include border screening.

REFERENCES:

1. ANSI N42.48- *American National Standard Performance Requirements for Spectroscopic Personal Radiation Detectors (SPRDs) for Homeland Security.* IEEE (New York) May 2018.
2. Bürkle, A., Segor, F. & Kollmann, M. J (Jan. 2011) Towards Autonomous Micro UAV Swarms.
    a. *Journal of Intelligent & Robotic Systems*. Volume 61, Issue 1–4, pp 339–353.
3. Cortez, R. A. (2008, Sept.). Smart Radiation Sensor Management. *IEEE Robotics & Automation Magazine*, pp. 85 - 93.

KEY WORDS: radiation, search, optimal, automated, unmanned aerial vehicles

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