U.S. Department of Homeland Security (DHS) Small Business Innovation Research

(SBIR) Program

THIS IS A PRE-SOLICITATION
DHS IS NOT SEEKING PROPOSALS AT THIS TIME

Due Date: See Section 3.8

Issued By:
DHS Office of Procurement Operations on behalf of:
The DHS Small Business Innovation Research (SBIR) Program

1.0 PROGRAM DESCRIPTION

1.1 Summary

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 Office's (CWMD) SBIR Program, invites small business concerns (SBCs) to review this Pre-Solicitation for awareness of the upcoming 23.1 DHS SBIR Solicitation.

The DHS SBIR Program Office encourages all small business concerns, including small disadvantaged, women-owned, veteran-owned, service-disabled veteran-owned, and socially and economically disadvantaged small business concerns, with the capability to conduct research and development for homeland security-related topic areas described in **Appendix A**, and to commercialize the results of that R/R&D, to submit proposals in response to topics described in the 23.1 Solicitation.

IMPORTANT:

- Please read this Pre-Solicitation carefully. This Pre-Solicitation is being provided for planning purposes, to allow SBCs to become familiar with the requirements for the upcoming 23.1 Solicitation. Failure to comply with the requirements in the 23.1 Solicitation will likely result negatively in the proposal evaluation or elimination from consideration for award. The final 23.1 Solicitation may differ from the Pre-Solicitation.
- This Solicitation contains topics for both the DHS SBIR Program and CWMD's SBIR Program. **Section 7.0** outlines the Seven (7) research topics – six (6) S&T topics and one (1) CWMD topic. Unsolicited proposals will not be accepted.
- While the Phase II proposal process is covered in this Solicitation, at this time **this Solicitation requests and accepts Phase I proposals only.** See **Section 1.3**.
- Prior to proposal submission, SBCs must register with the SBA Company Registration Database. See Section 2.1.
- SBCs that are majority-owned by multiple venture capital operating companies, hedge funds or private equity firms are NOT ELIGIBLE to submit proposals in response to the 23.1 Solicitation. See **Section 1.5**.
- Per the Small Business Administration (SBA) SBIR Policy Directive, dated October 1, 2020 (hereafter referred to as "the Policy Directive") to be eligible for a Phase I award, Offerors must meet or exceed the Phase II Transition Rate Benchmark, See **Section 3.7**, DHS Phase II Transition Rate Benchmark.

1.2 DHS SBIR Program, Purpose and Objectives

The statutory purpose of the SBIR Program is to strengthen the role of innovative small business concerns in Federally funded R/R&D. Program objectives are as follows:
(1) stimulate technological innovation;
(2) strengthen the role of small business concerns in meeting Federal R/R&D needs;
(3) foster and encourage participation by socially and economically disadvantaged small businesses (SDBs) and by women-owned small businesses (WOSBs); and
(4) increase private sector commercialization of innovations developed through Federal R/R&D, thereby increasing competition, productivity, and economic growth.

The federal SBIR Program is mandated by the Small Business Research and Development Act of 1982 (Public Law 97-219), the Small Business Research and Development Act of 1992 (Public Law 102-564), and the SBIR and STTR Extension Act of 2022 (Public Law 117-183).

The DHS SBIR Program follows the policies and practices of the Policy Directive. This Solicitation incorporates and uses the flexibility of the Policy Directive to encourage innovative proposals in response to the research topics listed in **Appendix A**.

1.3 Three Phase Program

The SBIR Program is a three-phase program. The objective of Phase I is to determine the scientific, technical, and commercial merit, feasibility of the proposed effort, and the SBC's quality of performance, with a relatively small agency investment prior to providing further Federal support in Phase II. Phase I proposals should concentrate on R/R&D which will significantly contribute to proving the scientific and technical feasibility, and commercialization potential of the proposed effort. The successful completion of Phase I is a prerequisite for further DHS support in Phase II. Offerors are encouraged to consider whether the R/R&D being proposed also has private sector potential, either for the proposed application or as a base for other applications.

The objective of Phase II is to continue the R/R&D effort from the completed Phase I. Phase II efforts further develop work from Phase I that meets program needs and exhibits potential for commercial application. Phase II is the principal R&D effort and is expected to produce a well-defined deliverable prototype. Phase II awards may be made to SBCs based on the results of their Phase I projects, and the scientific merit, technical merit, and commercialization potential of the Phase II proposal.

In accordance with the SBIR/STTR Reauthorization Act of 2016 (Public Law 114- 328), all small businesses awarded a Phase I contract originating from the 23.1 Solicitation are eligible to submit a Phase II proposal. A Contracting Officer will notify Phase I awardees with Phase II proposal submission requirements and deadlines.

SBIR Phase III refers to work that derives from, extends, or completes an effort made under prior SBIR funding agreements, but is funded by sources other than the SBIR Program. Phase III work is typically oriented towards commercialization of SBIR research or technology. Under Phase III, the SBIR awardee is expected to seek contracts and obtain funding from the private sector and/or the Federal government (non-SBIR federal government sources) to develop the prototype or supply goods or services related to the work performed under the SBIR contract(s) into a viable product or non-R&D service for sale in DHS and/or private sector markets.

A Phase III award, by its nature, is an SBIR award, has SBIR status, and must be accorded SBIR data rights. Phase III proposals can only be submitted by, and made to, a Phase I and/or Phase II awardee or successor in interest. The competition for SBIR Phase I and Phase II awards satisfies any competition requirement of the Armed Services Procurement Act, the Federal Property and Administrative Services Act, and the Competition in Contracting Act. Therefore, an agency that wishes to fund an SBIR Phase III project is not required to conduct another competition in order to satisfy those statutory provisions.

1.4 Key Dates and Events

The following chart shows the projected important events and corresponding dates of the 23.1 DHS SBIR Solicitation:

KEY DATES*	
EVENT	**DATE***
Pre-Solicitation issued:	November 17, 2022
Direct questions to Topic POC permitted:	November 17, 2022 – December 14, 2022
Solicitation released:	December 15, 2022
Phase I proposals submission:	December 15, 2022 – January 17, 2023
Questions for public response:	January 4, 2023,1:00 pm, ET
Q&A Posted on SAM.gov	January 10, 2023
Deadline for receipt of proposals:	January 17, 2023, 1:00 pm, ET
Phase I POP (5 months):	May 2023 – Oct 2023
Phase II Proposals Due:	~October 2023
Phase II Begins:	~March 2024
*The dates in the table above are approximate dates and are subject to change without notice.	

1.5 Eligibility

Not eligible - SBCs that are majority-owned by multiple venture capital operating companies, hedge funds or private equity firms are not eligible to submit proposals in response to the 23.1 Solicitation nor are they eligible to receive a DHS SBIR award.

To receive SBIR funds, each awardee of a Phase I or Phase II award must qualify as an SBC at the time of award and at any other time set forth in SBA's regulations at 13 CFR 121.701 through 121.705.

Small business concerns must register with the SBA Company Registration Database. See **Section 2.1.**

For both Phase I and Phase II, the primary employment of the principal investigator must be with the SBC at the time of the award and during contract performance. Primary employment means that more than one-half of the principal investigator's time is spent in the employ of the SBC. This precludes full-time employment with another organization.

For both Phase I and Phase II, all research or research and development must be performed by the SBC and its subcontractors in the United States in accordance with **Section 5.8** Research and Analytical Work.

1.6 SBIR Office Contacts

For general questions about the S&T Directorate's SBIR Program, please contact STSBIR.PROGRAM@hq.dhs.gov. For general questions about the CWMD SBIR Program, please contact CWMD.SBIR@hq.dhs.gov.

1.7 Definitions

Definitions provided in the Policy Directive and the Federal Acquisition Regulation (FAR) apply for the purposes of this Solicitation. Terms that are unique to the SBIR Program, this specific SBIR Solicitation, or may be unfamiliar to SBCs, are defined in **Appendix B**.

1.8 Fraud, Waste and Abuse

DHS and the SBIR Program Office are taking proactive measures to reduce the vulnerability of the SBIR Program to fraud, waste, and abuse. Instructions on the DHS OIG SBIR Fraud, Waste and Abuse training package will be included in the full Solicitation. Offerors must review the training package prior to submission of proposals.

To report SBIR fraud, please contact the DHS Office of the Inspector General (OIG):

DHS Office of Inspector General/MAIL STOP 0305
Attn: Office of Investigations - Hotline
245 Murray Lane SW
Washington, DC 20528-0305

Online: Allegation Form: https://hotline.oig.dhs.gov/#step-1

Call: 1-800-323-8603 toll free

TTY: 1-844-889-4357 toll free
To reach someone within S&T's SBIR Program Office about fraud, waste and abuse, please contact DHS S&T SBIR Program PM, STSBIR.PROGRAM@hq.dhs.gov.

To reach someone within the CWMD SBIR Program Office about fraud, waste and abuse, please contact the DHS CWMD SBIR PM at CWMD.SBIR@hq.dhs.gov.

2.0 REGISTRATION, CERTIFICATIONS, DATA COLLECTION, DISCLOSURE

2.1 Mandatory Registrations

In order to prepare and submit SBIR proposals to DHS under the 23.1 Solicitation, Offerors must be registered in the DHS SBIR Portal at https://sbir.dhs.gov/sbir/public.

Company registration is also required in the U.S. Small Business Administration's (SBA). Company Registry Database at http://sbir.gov/registration.
Prior to submitting the complete proposal to DHS, each Offeror must:

1. Affirm registration in the SBA Company Registry;
2. Input the company's SBC Control ID number in the Company Data section of the DHS SBIR Cover Sheet;
3. Upload a copy of the Registration (see Section 3.1).

PROPOSALS WHICH FAIL TO COMPLY WITH THE ABOVE REQUIREMENT ARE NON- RESPONSIVE AND WILL NOT BE CONSIDERED FOR AWARD.

Before an SBIR contract can be awarded, proposing firms must also be registered in the System for

Award Management (SAM). SAM is the official U.S. Government system that consolidated the capabilities of the Central Contractor Registration (CCR)/Federal Register, Online Representations and Certifications Application (ORCA), and the Excluded Parties List System (EPLS) databases. Although not required at the time of proposal submission to the DHS SBIR Program, it is highly recommended that Offerors register in SAM during the proposal process. Award cannot be made to a company unless they are registered in SAM. To register in SAM and/or update company's records, visit https://www.sam.gov/SAM/

Offerors are encouraged, but not required, to have a UEI (Unique Entity ID) number and a CAGE code at the time of proposal submission. Companies must obtain these before a contract can be awarded to the company. To obtain a UEI number, register with SAM.gov. Home CAGE Codes will be assigned by DLA during the registration process in SAM.gov. For more information about the Commercial and Government Entry (CAGE) code, please visit www.fsd.gov.

2.2 Required Certifications

At the time of proposal submission, each SBC must certify via the Cover Sheet of the proposal that it meets the size, ownership, and other requirements of the SBIR Program. In addition, the Policy Directive includes certifications requirements set forth in the SBIR/STTR Reauthorization and Improvement Act of 2016. The certifications require SBCs to certify that they are meeting the Program's requirements at award and during the life cycle of the funding agreement.

The DHS SBIR Programs will implement the certifications as follows:

1. SBIR Funding Agreement Certification – Time of Award (**Attachment 1**) – If selected for award, this certification will be provided by the Contracting Officer to the small business concern for completion prior to issuing the Phase I and Phase II award.
2. SBIR Funding Agreement Certification – Life Cycle Certification (**Attachment 2**) - The Life Cycle Certification will be included in resultant Phase I and Phase II contracts and is considered a deliverable.

2.3 Data Collection Requirement

Each Phase I and Phase II applicant is required to either enter information into SBA's database at www.SBIR.gov or to update previously entered information. Companies should login to www.SBIR.gov using the account created when registering for the SBA company registry database. The following are examples of data to be entered into the database:

- Any business concern or subsidiary established for the commercial application of a product or service for which an SBIR award is made.
- Revenue from the sale of new products or services resulting from the research conducted under each Phase II award.
- Additional investment from any source, other than Phase I or Phase II awards, to further the research and development conducted under each Phase II award.

The SBC may apportion sales or additional investment information relating to more than one Phase II award among those awards if it notes the apportionment for each award.

In addition, each Phase II awardee is required to update the appropriate information on the award

in the database upon completion of the last deliverable under the funding agreement and is requested to voluntarily update the information in the database annually thereafter for a minimum period of 5 years.

2.4 DISCLOSURE

Section 4(c) of the SBIR and STTR Extension Act of 2022 (P.L. 117-183) requires each small business concern submitting a proposal or application for a federally funded award to disclose information in the proposal or application regarding ties to the People's Republic of China and other foreign countries of concern. DHS will provide the disclosure form(s) with any instructions prior to the proposal submission deadline. The small business concern must complete the form(s) in accordance with any instructions and include the form(s) in the concern's proposal submission. Details on the requirements of the act can be found at https://www.congress.gov/bill/117th-congress/senate-bill/4900/text.

3.0 PROPOSAL PREPARATION INSTRUCTIONS AND REQUIREMENTS

3.1 Proposal Preparation and Length of Proposal

Offerors responding to the 23.1 Solicitation must submit a direct, concise, and informative research or research and development proposal. Each complete proposal must be submitted via the DHS SBIR Portal at https://sbir.dhs.gov/sbir/public.

The SBC will need to submit all the mandatory proposal sections. Some sections will be generated by the proposal submission portal and some will require a PDF upload (CWMD topic will also require documents submitted via email). Some sections which require PDF upload have a page limit.

The table below describes each mandatory section and, when applicable, page limitations. Proposals submitted which do not contain all mandatory sections and/or exceed page limitations as described in the table below, will be deemed **NON-RESPONSIVE** and will not be evaluated. Any attachments and appendices will be counted toward the page limitation. It is the responsibility of the SBC to ensure that once the proposal is submitted and uploaded into the system, it complies with the page limits. Only information included in the proposal submission will be considered for evaluation purposes; no referenced materials will be considered.

Mandatory Proposal Requirements		Phase I	Phase II
System Generated	Cover Sheet	As generated by system	
	Cost Proposal	As generated by system	
PDF Uploads	Technical Proposal	Limited to 20 pages	Limited to 40 pages
	Briefing Chart[1]	Limited to 1 page	Limited to 1 page
	SBA Company Registration	Limited to 1 page	Limited to 1 page
	Commercialization Report	N/A	No page limit – if applicable
Email Submissions	Non-disclosure Agreement[2]	CWMD Topics ONLY	CWMD Topics Only NDA from Phase I applies to Phase II

[1] Briefing Chart Template is Attachment 3 in the Solicitation.

[2] CWMD Topics ONLY – NDA must not be included in the proposals but submitted separately via provided email: see Section 4.3.

The Cover Sheet and the Cost Proposal are completed electronically via the DHS SBIR online proposal submissions system, while the Technical Proposal, Briefing Chart, SBA Company Registration, and the Commercialization Report, if applicable, are uploaded as PDF documents.

3.2 Proposal Cover Sheet, Technical Abstract, Project Aims, and Summary of Results

It is a requirement for the Offeror to provide basic details about the proposed effort on the proposal Cover Sheet. Additionally, the Cover Sheet includes the following fillable sections: Technical Abstract, Project Aims, and Summary of Results.

The Technical Abstract is limited to 250 words. The abstract must identify the purpose of the work and briefly describe the work to be carried out, the finding or results, and the potential commercial applications of the effort. If the Offeror's proposal is selected for award, the Technical Abstract section will be publicly posted on the DHS SBIR website and on the SBA's website; therefore, do not include proprietary or classified information in the Technical Abstract section of the Cover Sheet.

The Project Aims section is limited to 500 words, the Offeror should state the specific objectives of the research and development effort, define the proposed product, process or service to ultimately be developed. This section is intended for internal Government use and it will not be released.

For Phase I proposals only, the Offeror should state the specific objectives of the Phase I R/R&D effort, including the technical questions the Offeror will answer to determine the Phase I feasibility of the proposed approach and the impact that the results of the proposed research will exert on the research field(s) involved. The Offeror should state concisely and realistically what the proposed research is intended to accomplish in terms of its potential for technological innovation and commercial application. The proposed product, process or service that will ultimately be developed must be defined. Milestones for each of the aims should be included, as these will be used in the evaluation process.

For Phase II proposals only, the Offeror should state the specific objectives of the Phase II research and development effort including the impact that the results of the proposed research will exert on the research field(s). The Offeror should state concisely and realistically what the proposed research is intended to accomplish in terms of its potential for technological innovation and commercial application. The proposed product, process or service that will ultimately be developed must be defined. Milestones for each of the aims should be included, as these will be used in the evaluation process.

The Summary of Results section is limited to 500 words, must not contain proprietary information, and is for Government use only. The Offeror should provide the anticipated results and implications of the approach (both Phases I and II) and the potential commercial applications of the research.

3.3 Technical Proposal Format and Content

Prepare the Technical Proposal in single column format, 12-point Times New Roman, with 1" margins on 8 ½" x 11" paper. Company name, topic number, and proposal number must be

included in the header of each page. (The header may be included in the 1" margin.) The use of 10-point font is permissible for imbedded tables, figures, and graphics. See **Section 3.1** for page limitations for Phase I and Phase II proposals.

The Technical Proposal must be a single file, including tables, figures, graphics, and table of contents (if included). Do not lock, password protect, or encrypt the file to be uploaded. Perform a virus check before uploading the Technical Proposal file. If a virus is detected, it may cause rejection of the proposal.

The Technical Proposal must include the following sections in the order provided:

PROPOSAL FORMAT	
PHASE I PROPOSAL	**PHASE II PROPOSAL**
I. Identification and Significance of the Problem or Opportunity	I. Identification and Significance of the Problem or Opportunity
II. Phase I Technical Objectives	II. Phase I Technical Objectives and Results
III. Phase I Work Plan	III. Phase II Work Plan
IV. Related R/R&D	IV. Related R/R&D
V. Key Individuals and Bibliography of Directly Related Work	V. Key Individuals and Bibliography of Directly Related Work
VI. Relationship with Future R/R&D	VI. Relationship with Future R/R&D
VII. Commercialization Strategy	VII. Commercialization Plan
VIII. Facilities/Equipment	VIII. Facilities/Equipment
IX. Subcontractors/Consultants	IX. Subcontractors/Consultants
X. Potential Post Applications	X. Prior, Current, or Pending Support of Similar Proposals or Awards
XI. Prior, Current, or Pending Support of Similar Proposals or Awards	

The following is a brief description of each section of the Technical Proposal as applicable for each Phase:

- Identification and Significance of the Problem or Opportunity – Succinctly define the specific technical problem or opportunity addressed; the proposed innovation; the relevance and significance of the proposed innovation to a need(s) within the topic description; the proposed innovation relative to the state of the art; and the importance of the work proposed.

- Technical Objectives (**Phase I proposals only)** – State the specific objectives of the Phase I R/R&D effort, including the technical questions that must be answered to determine the feasibility of the proposed innovation/approach.

- Technical Objectives and Results (**Phase II proposals only)** – State the specific objectives of the Phase I R/R&D effort including the technical questions addressed to determine the feasibility. Address the progress, results and findings of the Phase I effort.

- Work Plan (**Phase I proposals only)** (including the efforts of the subcontractor(s)/consultant(s), if applicable) – Provide an explicit, detailed description of the Phase I approach. The Plan should indicate what tasks are planned, how, when, and where the work will be conducted, a schedule of

major events, and the final product(s) to be delivered. The Phase I effort should determine the technical feasibility of the proposed concept, and address the questions cited in the Technical Objectives immediately above. The methods planned to achieve each objective or task should be discussed explicitly and in detail. Task descriptions, schedules, resource allocations, estimated task hours for each key personnel and planned accomplishments, including project milestones, should be included. This section will be a substantial portion of the total Technical Proposal.

- Work Plan (**Phase II proposals only)** (including the efforts of the subcontractor(s)/ consultant(s), if applicable) – Provide an explicit, detailed description of the Phase II approach. The Plan should indicate what tasks are planned, how, when, and where the work will be conducted, a schedule of major events, the final product to be delivered, and the completion date of the effort. The Phase II effort should satisfy the anticipated results, as specified in the topic description. The methods planned to achieve each objective or task should be discussed explicitly and in detail. Task descriptions, schedules, resource allocations, estimated task hours for each key personnel and planned accomplishments, including project milestones, should be included. This section should be a substantial portion of the total proposal.

- Related Research/Research and Development – Describe significant (current and/or previous) R/R&D activities that are directly related to the proposed effort, including any conducted by the principal investigator, the Offeror, consultants, or others. Discuss any planned coordination with outside sources. Describe how these activities relate to the proposed project. Describe previous efforts similar but directly related to the proposed effort. For each effort, provide the following: (a) short description, (b) client for which work was performed (including individual to be contacted and phone number), and (c) date of completion. The Offeror should persuade reviewers of his or her awareness of key, recent R/R&D conducted by others in the specific topic area.

- Key Individuals and Bibliography of Directly Related Work – Identify key personnel who will be involved in the effort including information on directly related education, experience, and bibliographic information. A concise resume for the Principal Investigator and all key personnel, including a list of relevant publications (if any), should be included. All resumes will count toward the appropriate page limitation, see **Section 3.1**. **Offerors must identify any non-U.S. citizen(s) expected to be involved on proposed project** [including direct employees, subcontractors and consultants], their country of origin, type of visa or work permit under which they are performing, and an explanation of their anticipated level of involvement on this project. **Do not include Privacy Act Information**. SBC foreign national(s) must first be cleared by S&T's Foreign Disclosure Office prior to working and accessing data or information on awarded SBIR efforts. Foreign nationals must receive separate clearances for each award including awards from multiple topics and multiple awards on the same topic. All foreign nationals requiring SBIR access must complete DHS foreign access management screening. Foreign Nationals must complete the DHS Form, 11000-55 upon request during award negotiation.

- Relationship with Future Research/Research and Development (**Phase I proposals only)** – State the anticipated results of the proposed approach if the project is successful through Phase I and Phase II. Discuss the significance of the Phase I effort in providing a foundation for Phase II research or research and development effort, application and commercialization efforts (Phase III).

- Relationship with Future Research/Research and Development (**Phase II proposals only)**– State the anticipated results of the proposed approach if the project is successful through Phase II and

Phase III. Discuss the significance of the Phase II effort in providing a foundation for Phase III commercialization efforts.

- Commercialization Strategy (**Phase I proposals only)** – (1) Explicitly describe the company's strategy (vision) for commercializing the proposed technology and how it will transition to the specific operational component in DHS, other Federal Agencies, and/or private sector markets. (2) Provide specific information on what related technologies, if any, already exist in the market and why the technology being proposed will be superior and how this information was ascertained. (3) Include a discussion on the Offeror's current capability to commercialize previously developed technologies, as well as how the Offeror intends to develop the proposed technology all the way to the market. Responses to (1), (2), and (3) should be specific to the technology being proposed. Failure to respond to any of the items listed will result in a lower valuation for criterion c (See **Section 4.1** for Phase I evaluation criteria). If the Offeror has no commercial experience (item (3)) this should clearly be stated, and Offeror should describe how Offeror intends to bring the necessary experience to the company.

- Commercialization Plan (**Phase II proposals only)** – The Commercialization Plan should address the following: (Failure to address each item listed below in some detail will result in a lower valuation for criterion b (See **Section 4.1** for Phase II evaluation criteria):

a. *Company Information*. Focused objectives/core competencies; specialization area(s); products and significant product sales; and history of previous Federal and non-Federal funding, regulatory experience, and subsequent commercialization. Does the Offeror have marketing expertise and, if not, how does the Offeror intend to bring that expertise into the company?
b. *Customer and Competition*. Provide a clear description of key technology objectives, current competitors, and advantages (cost and technical) compared to competing products or services, description of hurdles to acceptance of the innovation. Address who the customers will be, and for non-DHS customers explain the demand drivers for this technology. Estimate the market size. Has the Offeror contacted anyone in the projected target customer base including DHS customers? Identify potential factors that could have positive and/or negative impacts regarding the transition of the proposed product.
c. *Market*. Provide milestones, target dates, analyses of market size, and the estimated market share after first and five-year sales. Provide detailed explanation on the plan to obtain market share.
d. *Financing*. Provide detailed information on the identification and acquisition of costs associated in transitioning the proposed product/services into the market. If available, provide brief discussion on potential financial sources. What are the plans for securing necessary funding for Phase III?
e. *Intellectual Property (IP)*. Provide a detailed description on how the company plans to acquire and protect appropriate IP of the proposed product/service. What is the IP strategy and how will it be protected? Address patent status, technology lead, trade secrets or other demonstrations of a plan to achieve sufficient protection to realize the commercialization stage and attain at least a temporal competitive advantage.
f. *Assistance and Mentoring*. Provide plans for securing needed technical or business assistance through mentoring, partnering, or through arrangements with state assistance programs, small business development centers, Federally funded research laboratories, Manufacturing Extension Partnership centers, or other assistance providers. Address how the product will be produced.

The Commercialization Plan should also include a schedule and the basis for that schedule showing the quantitative results from the Phase II project that the company expects to report in its Company Commercialization Report Updates one year after the start of the Phase II, at the

completion of Phase II, and after the completion of Phase II (i.e., amount of additional investment, sales revenue, etc.).

- Facilities/Equipment – Provide information to allow the evaluators to assess the ability of the Offeror to carry out the activities of the proposed phase as well as all subsequent phases. Describe available instrumentation and physical facilities necessary to carry out the proposed effort. Equipment to be purchased, as detailed in the Cost Proposal, should be justified under this section. Also state whether the facilities where the proposed work will be performed meet environmental laws and regulations of federal, state, and local governments for, but not limited to, the following groupings: airborne emissions, waterborne effluents, external radiation levels, outdoor noise, solid and bulk waste disposal practices, and handling and storage of toxic and hazardous materials.

- Subcontractors/Consultants – Involvement of any subcontractor(s) or consultant(s) (including Federal Laboratories, FFRDCs, universities, and technical assistance providers) is permitted. If such involvement is proposed, it should be described in detail in this section and in the Cost Proposal. Subcontractors' or consultants' involvement under Technical and Business Assistance (see **Section 5.11**) should be clearly delineated from involvement by other subcontractors and consultants. A minimum of two-thirds of the research and/or analytical work in Phase I, as measured by total contract value, should be carried out by the proposing SBC. A minimum of one-half of the research and/or analytical work in Phase II, as measured by total contract value, should be carried out by the proposing SBC. If the SBC determines that it needs to acquire services from a non-U.S. source, it must fully explain in its proposal why a non-U.S. source must be used, and why no qualified U.S. source exists to perform the same services.

- Potential Post Applications – Briefly describe the following: (1) whether and by what means the proposed project appears to have potential commercial application; and (2) whether and by what means the proposed project appears to have potential use by the Federal Government.

- Prior, Current, or Pending Support of Similar Proposals or Awards – WARNING – While it is permissible, with proposal notification, to submit identical proposals or proposals containing a significant amount of essentially equivalent work (see **Appendix B**) for consideration under numerous Federal program solicitations, it is unlawful to enter into funding agreements (contracts or grants) requiring essentially equivalent effort. If there is any question concerning this, it must be disclosed to the soliciting agency or agencies before award.

  If an Offeror elects to submit identical proposals or proposals containing a significant amount of essentially equivalent work in response to the 23.1 Solicitation, or other Federal program solicitations, or is substantially the same as another proposal that has been funded, is now being funded, will be submitted to other agencies for funding consideration, or is pending with DHS or another Federal Agency, the Offeror must indicate so on the Proposal Cover Sheet and provide the following information in the Technical Proposal:

a. Name and address of the Federal Agency(s) to which a proposal was submitted, will be submitted, or from which an award is expected or has been received
b. Date of proposal submission or date of award
c. Title of proposal
d. Name and title of principal investigator or project manager for each proposal submitted or award received

e. Title, number, and date of solicitation(s) under which the proposal was submitted, will be submitted, or under which award is expected or has been received
f. If award was received, state contract number
g. Specify the applicable topics for each SBIR Proposal submitted or award received

Note: If this section does not apply, the following statement should be included in the Technical Proposal: "No prior, current, or pending support for proposed work."

3.4 Cost Proposal

All Offerors must submit a cost proposal via as part of the submission to the SBIR Portal at https://sbir.dhs.gov/sbir/public. Proposed costs must not exceed the maximum thresholds outlined below.

SBIR Topic Proposal Structure*

Phase I	Phase II
$150,000**	$1,000,000***
5 months	24 months

Notes: * Proposal Structure may be modified in 23.1 Solicitation or in Phase II Proposal Submission Instructions.

Phase I total is not inclusive of Discretionary Technical and Business Assistance. If requesting assistance, the potential total is $150K plus assistance. Please see **Section 5.11

***Phase II total IS inclusive of the Discretionary Technical and Business Assistance. If requesting assistance, the total must not exceed $1M. Please see **Section 5.11**.

For additional information on the items in the Cost Proposal, reference Section 4.3.2 of the *Portal Registration and SBIR Submission Guide* located under "Resources" at https://sbir.dhs.gov/sbir/public.

Additionally, more information about cost proposals and accounting standards can be found on the DCAA customer guidance page, available at https://www.dcaa.mil/Customers/Guidance/

Proposals submitted under the 23.1 Solicitation will be considered valid for 180 days. If a proposal is selected for award, Offerors should be prepared to submit further cost/pricing documentation to the Contracting Officer in order to justify items on the cost proposal.

The following are required elements of the cost proposal:

- Direct Labor – list the name, labor category, labor hours and labor rate of each employee working on the project
- Overhead Cost – specify the current overhead rate. Use overhead rate approved by a cognizant federal agency, if available.
- Other Direct Cost – include direct material, special testing, equipment, travel, subcontracts, etc.

For Phase I planning purposes, Offerors should budget for two mandatory trips to Washington, DC – a post-award conference and a one-day meeting to present the results in the final report. In the event that an in-person post award conference is not feasible, then a virtual event will take place.

The structure of the post award conference is different for S&T and CWMD topics. Refer to the table below for details:

PHASE I POST AWARD DETAILS		
Day	S&T Topics	CWMD Topics
1	(Mandatory) Session includes: Program background and contracting overview One-on-One sessions with Topic Managers	(Mandatory) Session includes: Program background and contracting overview One-on-One sessions with Topic Managers
2	(Mandatory) Commercialization workshop	N/A
3	(Optional) Showcasing and Presentation Workshop - venue where small business concerns can enhance their presentation skills in front of Government, Industry, and representatives from the investment community	N/A

3.5 Briefing Chart

The mandatory one-page Briefing Chart should provide a very concise summary of the overall effort. The Briefing Chart is uploaded during proposal submission and may be used in the evaluation process. The briefing chart MUST NOT contain proprietary or classified data. Offerors must use the Briefing Chart template provided in **Attachment 3**.

3.6 Commercialization Report

All Phase II Offerors with previous Phase II awards from any federal agency must submit a Commercialization Report. It is important to note that this is a separate document from the Commercialization Plan required as part of the Phase II Technical Proposal.

Offerors that have not received any Phase II awards should check the appropriate box on the Cover Sheet certifying that the company has not received SBIR Phase II funding from any agency. Offerors with no prior Phase II awards will not be negatively impacted in the evaluation process. Instead, such companies will be evaluated based on the Commercialization Plan, see **Section 3.3**.

If applicable, the succinct Commercialization Report should be in PDF format and submitted as a separate upload during the Phase II proposal submission. The following are examples of company commercialization data expected in the Commercialization Report:

- Any business concern or subsidiary established for the commercial application of a product or service for which an SBIR award is made.
- Revenue from the sale of new products or services resulting from the research conducted under each Phase II award; delineate revenue by government, open market, prime contractors, other awards, and when this revenue event occurred.

- Additional investment from any source, other than Phase I or Phase II awards, to further the research and development and/or commercialization conducted under each Phase II award.
- Whether the Phase II technology has been used in a fielded DHS system or acquisition program, and, if so, which system or program.
- The number of patents resulting from the contractor's participation in the SBIR Program and whether any licenses based on these patents have been issued.
- Whether the company has completed an initial public offering (IPO) of stock, merged or been acquired resulting, in part, from any DHS SBIR Phase II project.

The Commercialization Report for any prior Phase II award received by the company must be current as of the end of the company's last full fiscal year (FY). The company may apportion sales or additional investment information relating to more than one Phase II award among those awards, if it notes the apportionment for each award.

3.7 DHS Phase II Transition Rate Benchmark

The Phase I to Phase II Transition Rate requirement applies only to SBIR and STTR Phase I applicants that have received more than 20 (21 or more) Phase I awards over the past 5 fiscal years, excluding the most recent year. These companies must meet the required benchmark rate of transition from Phase I to Phase II. The current Transition Rate requirement, agreed upon and established by all 11 SBIR agencies and published for public comment at 77 FR 63410 (https://www.federalregister.gov/documents/2012/10/16/2012-25328/sbirsttr-phase-i-to-phase-ii-transition-benchmarks) in October 2012 and amended at 78 FR 30951 (https://www.federalregister.gov/documents/2013/05/23/2013-12312/sbirsttr-phase-i-to-phase-ii-transition-benchmarks) in May 2013, is that an awardee must have received an average of one Phase II for every four Phase I awards received during the most recent 5-year time period (which excludes the most recently-completed fiscal year) to be eligible to submit a proposal for a new Phase I (or Direct-to-Phase II) award. That is, the ratio of Phase II to Phase I awards must be at least 0.25.

For SBIR/STTR awardees that have received more than 20 Phase I awards during the time period, SBA calculates the company Transition Rate and displays it on the company registry page at www.sbir.gov. Companies with less than that number of past Phase I awards will only see "N/A" because the benchmark requirement does not apply to them. To calculate the company Transition Rate, SBA divides the total number of SBIR and STTR Phase II awards a company received from all agencies during the past 5 fiscal years by the total number of SBIR and STTR Phase I awards it received during the past 5 fiscal years excluding the most recently-completed year. The 5-year period over which Phase I awards are counted excludes the most recently completed fiscal year because not all Phase II awards can occur within the same year as the Phase I award.

3.8 Questions

General Questions
Questions pertaining to the S&T's SBIR Program should be submitted to STSBIR.PROGRAM@hq.dhs.gov.

Questions pertaining to the CWMD's SBIR Program should be submitted to CWMD.sbir@hq.dhs.gov.

Technical Questions

The Pre-Solicitation period is from November 17, 2022 through December 15, 2022
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 23.1 Pre-Solicitation SBIR Topic Areas.
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 are limited to technical information related to improving the understanding of a topic's requirements. Any questions or inquiries seeking advice or guidance on a solution approach are unacceptable and will not receive a response.
No further contact between offerors and Technical Points of Contact shall occur after 5pm on December 15, 2022.
Rules for submitting questions after Pre-Solicitation ends, on December 15, will be outlined in the 23.1 Solicitation.
The Government anticipates releases of the 23.1 Solicitation on December 15, 2022.
Electronic Submission Questions.

Questions about the electronic submission of proposals should be submitted to the Help Desk at (571) 446-4869, or via email to OIPPortalHelpDesk@hq.dhs.gov. The Help Desk may be contacted from 9:00 a.m. to 5:00 p.m. ET, Monday through Friday excluding Federal Holidays.

4.0 METHOD OF SELECTION AND EVALUATION CRITERIA

4.1 Evaluation Criteria, Factors and Ratings

The **Phase I evaluation criteria**, listed in decreasing order of importance, are as follows:

a. Technical Merit – the soundness, technical merit, and innovation of the proposed approach and its incremental progress toward topic or subtopic solution.

b. Staff Qualifications and Capability – the qualifications of the proposed principal investigator, key personnel, supporting staff, and consultants. Qualifications include the ability to perform the research and development.

c. Potential for Commercialization – the potential for commercial application, either in the Government or private sector, and the benefits expected to accrue from this commercialization.
d. Cost/Price The reasonableness of the cost proposal. The evaluation of cost/price will include whether the level of effort and other direct costs are appropriate for the proposed work.

The **Phase II evaluation criteria**, listed in decreasing order of importance, are as follows:

a. Technical Merit – the soundness, technical merit, and innovation of the proposed approach and its incremental progress toward topic or subtopic solution.

b. Potential for Commercialization – the potential for commercial application, either in the Government or private sector, and the benefits expected to accrue from this commercialization. *The lack of a Company Commercialization Report, due to the offeror having no prior Phase II awards, will not affect its ability to receive an award.*

c. Staff Qualifications and Capability – the qualifications of the proposed principal investigator, key personnel, supporting staff, and consultants. Qualifications include the ability to perform the research and development.

d. Cost/Price – The reasonableness of the cost proposal. The evaluation of cost/price will include whether the level of effort and other direct costs are appropriate for the proposed work.

Evaluators will assess the strengths, weaknesses, and deficiencies of the above criteria using the following definitions:

a. Strength – An aspect of the proposal that benefits the Government in terms of the quality of the Offeror's performance, cost effectiveness, or reduced risk towards successful contract performance.

b. Weakness – A flaw in the proposal that decreases the likelihood successful contract performance. A "significant weakness" is a flaw that dramatically increases the risk of unsuccessful contract performance. When weaknesses are identified, the Government will provide comment(s) on the significance of the weakness.

c. Deficiency – A material failure of a proposal that would result in an unacceptable risk level of contractor performance.

Evaluators will use one of the following adjectival ratings for each of the Technical Merit, Staff Qualifications and Capability, and Potential for Commercialization criterion:

a. Excellent – The proposal demonstrates a superior understanding of the requirements and an approach that significantly exceeds all topic objectives. Proposal has exceptional strengths that will significantly benefit the Government and risk of unsuccessful performance is very low.

b. Very Good – Offeror's proposed approach is likely to satisfy most of the topic objectives and shows a high probability of successful contract performance. Offeror's proposal has strengths that will benefit the Government and one or more weaknesses, but no significant weaknesses.

c. Good – Offeror's proposed approach has a reasonable likelihood of satisfying the topic objectives and shows a good probability of successful contract performance. Offeror's proposal has some strengths that will benefit the Government, and some weaknesses.

d. Fair – Offeror's proposed approach is unlikely to meet the topic objectives and shows a low probability of successful contract performance. Offeror's proposal has weaknesses, some that may be significant, and few strengths, if any, that will benefit the Government.

e. Unacceptable – The Offeror's proposed approach fails to meet the topic objectives and requirements.

The Cost/Price criterion is not adjectively rated as outlined above; rather, the evaluation team will determine if the cost proposal is either acceptable or unacceptable as defined below:

a. Acceptable - The proposed cost elements, including labor mix, labor hours, material, special testing,

special equipment, travel, subcontracts, if applicable, are appropriate for the proposed effort.

b. Unacceptable - The proposed cost elements, including labor mix, labor hours, material, special testing, special equipment, travel, subcontracts, if applicable, are not appropriate for the proposed effort.

4.2 Proposal Review Feedback

DHS will make award decisions, and notify applicants of its decisions, within 90 calendar days from the closing date of the 23.1 Solicitation. Specific instructions on requesting feedback will be provided to each Offeror upon notification that their proposal was not selected for award.

Requests for proposal feedback must be received within three (3) business days of the notification and will only be provided to Offerors upon request.

4.3 Contractor Support Services in Support of the Selection Process

Offerors are advised that non-federal, contract support personnel will be used to carryout administrative functions for the SBIR Program Office and topic program managers. The contract support personnel will have access to proposals. Administrative duties may include, but are not limited to, making and distributing copies of proposal, scheduling and attending meetings, taking and compiling notes, etc.

In addition to administrative functions, CWMD will use contractor support (Mayvin, Inc.) as advisors in the source selection process. In accomplishing their duties related to the source selection process, the contractor support may require access to proprietary information contained in the Offerors' proposals. Therefore, pursuant to FAR 9.505-4, this firm must execute an agreement with each Offeror that states that they will (1) protect the Offerors' information from unauthorized use or disclosure for as long as it remains proprietary and (2) refrain from using the information for any purpose other than that for which it was furnished.

For Topic DHS231-007, each Offeror must contact the contractor support company to effect execution of a non-disclosure agreement. CWMD highly recommends that the offeror contacts the contractor support company at least two weeks prior to the proposal submission deadline to initiate such an agreement.

CWMD highly recommends that the Offerors use the standard one-page company-to-company, non-disclosure agreements found in Attachment 4. It is imperative that Offerors submitting proposals for Topic DHS231-007 submit a copy of their signed agreement to CWMD.SBIR@hq.dhs.gov. **Proposals submitted to this topic will not be considered complete until the submission of the dually signed non-disclosure agreement. Failure to execute such an agreement with the above company will result in the Offeror's proposal submission being found non-compliant. Non-compliant submissions will not be reviewed or evaluated.**

5.0 CONSIDERATIONS

5.1 Awards

While it is the intent of the DHS SBIR Program to award a negotiated contract for each proposal selected, selection does not guarantee award. No contracts will be awarded until all relevant proposals submitted in response to a specific topic have been evaluated and an award decision

rendered. The number of SBIR Phase I and Phase II awards will be consistent with the SBIR budget. The number of Phase I awards is estimated to be 21. All DHS SBIR awards resulting from the 23.1 Solicitation will be posted at https://sbir.dhs.gov/sbir/public.

A firm-fixed price (FFP) contract will be awarded for all Phase I awards. Phase II contracts will be awarded as a cost-plus fixed-fee (CPFF) contract. In accordance with FAR 16.301-3, to award a CPFF contract, Offerors must have an accounting system that is adequate for determining cost applicable to the contract.

5.2 Reports and Deliverables

At a minimum, monthly reports (both Phase I and Phase II) and a final comprehensive report (both Phase I and Phase II) will be required in all SBIR awards. See topic write up for further details on additional deliverables.

In addition, if you are proposing and awarded a contract with Technical and Business Assistance an additional report is required (see **Section 5.11).**

Other deliverables appropriate to the proposed effort will be identified in the topic area description. Phase I and II awardees will be required to submit the *SBIR Funding Agreement Certification – Life Cycle Certification* (**Attachment 2**) during the contract period of performance.

5.3 Invoice Instructions

The specific invoicing instructions will be incorporated into the contract upon completion of negotiations between the Government and the successful Phase I or Phase II Offeror.

5.4 Innovations, Inventions and Patents

Proprietary Information. Information contained in unsuccessful proposals will remain the property of the applicant. The Government will, however, retain copies of all proposals. Public release of information in any proposal submitted will be subject to existing statutory and regulatory requirements.

If proprietary information is provided by an applicant in a proposal, which constitutes a trade secret, proprietary commercial or financial information, confidential personal information or data affecting the national security, it will be treated in confidence, to the extent permitted by law. This information must be clearly marked by the applicant with the term "proprietary information" and the following legend must appear on the title page of the proposal:

"These data shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed in whole or in part for any purpose other than evaluation of this proposal. If a funding agreement is awarded to this applicant as a result of or in connection with the submission of these data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the funding agreement and pursuant to applicable law. This restriction does not limit the Government's right to use information contained in the data if it is obtained from another source without restriction. The data subject to this restriction are contained on pages___of this proposal."

DHS assumes no liability for inadvertent disclosure or use of unmarked data. The Government will limit dissemination of such proprietary information to within official channels.

Marking of Proprietary Information. To properly mark proprietary information on the proposal, use an asterisk (*) in the right and left margins on pages deemed proprietary. If all information on a page is deemed proprietary, include this statement, "ENTIRE PAGE IS PROPRIETARY," in both the header and footer of the associated page. Do not label the entire proposal "proprietary." All other markings (e.g., "Company Confidential", "Business Sensitive", etc.) will not be recognized.

Rights in Data Developed Under SBIR Funding Agreements.
SBIR Data, all Data developed or generated in the performance of an SBIR award, including Technical Data and Computer Software developed or generated in the performance of an SBIR or STTR award, is subject to the SBIR data protection period. Upon expiration of the protection period for SBIR Data, the Government has a royalty-free license to use, and to authorize others to use on its behalf, these Data for Government Purposes, and is relieved of all disclosure prohibitions and assumes no liability for unauthorized use of these Data by third parties. The Government receives Unlimited Rights in all Form, Fit, and Function Data, OMIT Data, and unmarked SBIR Data. Please see the Policy Directive update of October 1, 2020 for additional information.

If the Offeror's proposal is selected for funding, the Contracting Officer will contact the apparent awardee so that the apparent awardee has the opportunity to submit assertions in accordance with FAR clause 52.227-20. The assertions must be identified, and assertion of use, release, or disclosure must be provided for the government's review and acceptance. Contracts cannot be awarded until assertions have been approved.

Copyrights. With prior written permission of the Contracting Officer, the awardee normally may assert its copyright and publish (consistent with appropriate national security considerations, if any) material developed with DHS SBIR support. DHS receives a royalty-free license for the Federal Government and requires that each publication contain an appropriate acknowledgement and disclaimer statement.

Patents. Small business concerns normally may retain the principal worldwide patent rights to any invention developed with Government support. In such circumstances, the Government receives a royalty-free license for Federal Government use, reserves the right to require the patent holder to license others in certain circumstances, and may require that anyone exclusively licensed to sell the invention in the United States must normally manufacture it domestically. To the extent authorized by 35 U.S.C. 205, the Government will not make public any information disclosing a Government-supported invention for a minimum 4-year period (that may be extended by subsequent SBIR funding agreements) to allow the awardee a reasonable time to pursue a patent.

Invention Reporting. SBIR awardees must report inventions to the awarding agency within 2 months of the inventor's report to the awardee. Awardees must report inventions to DHS through the NIST iEdison Invention Reporting Systems at www.iedison.gov. Use of the iEdison System satisfies all invention reporting requirements mandated by 37 CFR Part 401, with particular emphasis on the Standard Patent Rights Clauses, 37 CFR 401.14.

5.5 Cost-Sharing

Cost-sharing is permitted for proposals under the 23.1 Solicitation; however, cost-sharing is not required and will not be considered in evaluation of proposals.

5.6 Profit or Fee

In accordance with FAR 15.404-4, Offerors may include a reasonable fee or profit consistent with R/R&D work.

5.7 Joint Ventures or Limited Partnerships

Joint ventures and limited partnerships are eligible provided that the entity created qualifies as a small business concern in accordance with the Small Business Act, 15 U.S.C. 631.

5.8 Research and Analytical Work

For Phase I, a minimum of two-thirds of the research and/or analytical work must be performed by the proposing small business concern. For Phase II, a minimum of one-half the research and/or analytical work must be performed by the proposing small business concern. Subcontract cost will be calculated as a percentage of the total contract value.

5.9 Awardee Commitments and Summary Statements

Upon award of an SBIR contract, the awardee will be required to make certain legal commitments through acceptance of numerous clauses in the Phase I and Phase II contracts. The outline that follows is illustrative of the types of clauses to which the contractor would be committed. This list is not a complete list of clauses to be included in Phase I funding agreements and is not the specific wording of such clauses. Copies of complete terms and conditions are available upon request.

a. *Standards of Work.* Work performed under the funding agreement must conform to high professional standards.
b. *Inspection.* Work performed under the funding agreement is subject to Government inspection and evaluation at all times.
c. *Examination of Records.* The Comptroller General (or a duly authorized representative) must have the right to examine any pertinent records of the awardee involving transactions related to this funding agreement.
d. *Default.* The Government may terminate the funding agreement if the contractor fails to perform the work contracted.
e. *Termination for Convenience.* The funding agreement may be terminated at any time by the Government if it deems termination to be in its best interest, in which case the awardee will be compensated for work performed and for reasonable termination costs.
f. *Disputes.* Any dispute concerning the funding agreement that cannot be resolved by agreement must be decided by the contracting officer with right of appeal.
g. *Contract Work Hours.* The awardee may not require an employee to work more than 8 hours a day or 40 hours a week unless the employee is compensated accordingly (for example, overtime pay).
h. *Equal Opportunity.* The awardee will not discriminate against any employee or applicant for employment because of race, color, religion, sex, or national origin.
i. *Affirmative Action for Veterans.* The awardee will not discriminate against any employee or application for employment because he or she is a disabled veteran or veteran of the Vietnam era.
j. *Affirmative Action for Handicapped.* The awardee will not discriminate against any employee or applicant for employment because he or she is physically or mentally handicapped.
k. *Officials Not To Benefit.* No Government official must benefit personally from the SBIR funding agreement.
l. *Covenant Against Contingent Fees.* No person or agency has been employed to solicit or secure the funding agreement upon an understanding for compensation except bona fide employees or

commercial agencies maintained by the awardee for the purpose of securing business.

m. *Gratuities.* The funding agreement may be terminated by the Government if any gratuities have been offered to any representative of the Government to secure the award.
n. *Patent Infringement.* The awardee must report each notice or claim of patent infringement based on the performance of the funding agreement.
o. *American Made Equipment and Products.* When purchasing equipment or a product under the SBIR funding agreement, purchase only American-made items whenever possible.
p. *Advertisements, Publicizing Awards, and News Releases*. All press releases or announcements about agency programs, projects, and contract awards must be cleared by the Contracting Officer's Representative (COR) and the Contracting Officer. Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity news release or commercial advertising without first obtaining explicit written consent to do so from the Program Manager/COR and the Contracting Officer. The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.
q. *E-Verify*. Contracts exceeding the simplified acquisition threshold may include the FAR clause 52.222-54 *"Employment Eligibility Verification"* unless exempted by the conditions listed at FAR 22.1803.
r. *Prohibition on Contracting with Inverted Domestic Corporation*. Section 835 of the Homeland Security Act, 6 U.S.C. 395, prohibits the Department of Homeland Security from entering into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation as defined in HSAR 3052.209-70. The Prohibition on Contracting with Inverted Domestic Corporation clause will be incorporated into awards resulting from the 23.1 Solicitation.

5.10 Release of Proposal Information

In submitting a proposal, the Offeror agrees to permit the Government to publicly disclose basic company information (e.g.- company size, company name, award amount, award date etc.) upon award. Other proposal data is considered to be the property of the Offeror, and DHS will protect it from public disclosure to the extent permitted by law including the Freedom of Information Act. Please note, in accordance with the Small Business Administration's SBIR Policy Directive, the DHS SBIR Office will provide the basic proposal information to the Small Business Administration's Application Information database at www.SBIR.gov, as identified in the Policy Directive.

In an effort to increase the transition of SBIR technologies and facilitate partnerships between small business concerns, large integrators, and program offices, the DHS SBIR Program Office may provide proposal information to the Department of the Navy's SBIR Program Office for inclusion in its Navy SBIR/STTR search database at www.navysbirsearch.com. Awardees who do not want their proposal to be included in this database must opt out by answering "No" on the Cover Sheet.

5.11 Discretionary Technical and Business Assistance (TABA)

Per the Policy Directive, SBC may request the authority to select their own TABA provider. The SBC must request TABA as a part of their proposal. If requested and approved, DHS SBIR will provide up to $6,500.00 during Phase I and $50,000 during Phase II, for Technical and Business

Assistance to an SBIR awardee. The Phase I funding thresholds ARE NOT inclusive of TABA allowance. Phase II thresholds ARE inclusive of TABA allowance, see Section 3.4. Regardless of whether the Offeror proposes TABA, the period of performance thresholds for the proposal remain the same.

In order for awardee TABA request to be approved, the request must comply with Section 9(b) of the Policy Directive. If approved, the awardee shall be required to comply with the reporting requirements from Section 9 (b) and may not be eligible to participate in the DHS provided TABA (referred to as the Commercialization Assistance Marketplace, see **Section 5.12**).

These subcontract costs must be clearly identified as TABA accounted for in the Cost Proposal; however, profit or fee, or indirect rates, shall not be applied to TABA. Offerors must provide a budget justification, an outline of the specific services technical assistance to be provided, and the detailed qualifications and experience of the proposed subcontractor/consultant being requested.

5.12 Commercialization Assistance Marketplace

Awardees may receive Commercialization Assistance through the DHS SBIR Program Office. The SBIR Program Office is under contract with a company that can provide commercialization assistance to Phase II awardees. If eligible, awardees will receive notification from the DHS SBIR Office on what services are available and how to obtain these services at no cost to the small business concern.

5.13 Classified Proposals

Classified proposals are NOT accepted under the DHS SBIR Program. Classified proposals will be appropriately destroyed upon receipt.

5.14 Animal and/or Human Subjects

Funds cannot be released or used for any portion of the project involving animal and/or human subjects until all the proper approvals have been obtained in accordance with applicable regulations. See **Appendix B** for more details concerning the use of Animal and/or Human Subjects.

5.15 Export Control

Offerors are advised that the export of any goods or technical data from the United States, and the disclosure of technical data to foreign nationals, may require some form of export license from the U.S. Government. Failure to obtain necessary export licenses may result in criminal liability of Offerors under U.S. laws.

Offerors are responsible for ensuring compliance with the International Traffic in Arms Regulations administered by the U.S. Department of State (22 C.F.R. Parts 120 to 130), Export Administration Regulations administered by the U.S. Department of Commerce (15 C.F.R. Parts 730 to 774), and Foreign Assets Control Regulations administered by the U.S. Department of Treasury (31 C.F.R. Parts 501 to 598), as warranted, and with compliance with all recordkeeping requirements under U.S. export regulations. Offerors are responsible for compliance with any applicable export license, reporting, or other preapproval requirements by the U.S. Government. DHS neither represents that a license or preapproval shall not be required nor that, if required, it shall be issued. Nothing granted herein to Offerors provides any such export license or other preapproval.

Offerors are asked to identify any anticipated export compliance issues in their response to the 23.1 Solicitation. Specifically, Offerors are advised to include information in their response regarding any known equipment, software or technical data that will be developed as a result of work to be performed under the 23.1 Solicitation that is subject to export control restrictions.

To the extent that export-controlled information may be provided to DHS by Offerors in response to a solicitation, Offerors are responsible for ensuring that such information is appropriately marked and are responsible for complying with all applicable export controls and regulations in the process of providing such information.

5.16 DHS SBIR Phase II Enhancement Programs

To further encourage the transition of SBIR-funded research into DHS acquisition programs as well as to the private sector, the DHS SBIR Program offer offers Cost Match.

Cost Match. The DHS S&T and CWMD SBIR Programs include a Cost Match feature for their respective SBIR projects that attract matching funds from an outside investor for the Phase II SBIR effort. The purpose of the cost match is to focus DHS SBIR funding on those projects that are most likely to be developed into viable new products that DHS and others will purchase and that will make a major contribution to homeland security and/or economic capabilities. The cost match can only occur during the Phase II period of performance.

Outside investors may include such entities as another company, a venture capital firm, an individual investor, or a non-SBIR government program; they do not include the owners of the small business concern, their family members, and/or affiliates of the small business concern. In order to be considered for DHS SBIR cost match, the outside investors must commit a minimum of $100,000. DHS will, at its discretion and subject to availability of funds, match up to 50% of funds received, for a maximum DHS SBIR contribution of $250,000.

The additional work proposed for the Cost Match feature should be an expansion of the technical work being performed in the Phase II project and must fall within the general scope of the present Phase II project.

5.17 Additional Information

This Pre-Solicitation is intended for informational purposes and reflects current planning. If there is any inconsistency between the information contained herein and the terms of any resulting SBIR funding agreement, the terms of the funding agreement are controlling.

Before award of an SBIR funding agreement, the Government may request the applicant to submit certain organizational, management, personnel, and financial information to assure responsibility of the applicant.

DHS shall not be liable for any costs incurred by the Offerors prior to award of any SBIR contract.

This Pre-Solicitation is not an offer by the Government and does not obligate the Government to make any specific number of awards. Also, awards under the SBIR Program are contingent upon the availability of funds.

If an award is made pursuant to a proposal submitted under the 23.1 Solicitation, a representative

of the contractor or grantee or party to a cooperative agreement will be required to certify that the concern has not previously been, nor is currently being, paid for essentially equivalent work by any Federal agency.

In the event that DHS has a need to share sensitive information with the SBIR awardee, the contractor must clear DHS suitability.

6.0 SUBMISSION OF PROPOSALS

Proposal due date will be contained in the 23.1 Solicitation. The estimated due date is January 17, 2023. This date is subject to change and SBCs interested in submitting proposals will need to verify the actual due date in the 23.1 Solicitation.

The DHS SBIR Programs use an electronic online proposal submission system located at https://oip.dhs.gov/sbir/public. All Offerors must submit proposals through this online system. Paper submissions and proposals received by any other means will not be accepted, evaluated, or considered for award.
Offerors are strongly encouraged to read the *Portal Registration and Submissions Training Guide* and follow the instructions for proposal submission. This guide can be found at https://sbir.dhs.gov/sbir/public under "Resources." The Guide provides step-by-step instructions for company registration and proposal submission.

Questions about the electronic submission of proposals should be submitted to the Help Desk. The Help Desk may be contacted at (571) 446-4869, or OIPPortalHelpDesk@hq.dhs.gov from 9:00 a.m. to 5:00 p.m. ET, Monday through Friday.

Late proposals will not be accepted or evaluated.

Note: As the close of the 23.1 Solicitation approaches, heavy traffic on the web servers may cause delays. Plan ahead and leave ample time to prepare and submit your proposal. Offerors bear the risk of website inaccessibility due to heavy usage in the final hours before the Solicitation closing time. In accordance with the FAR clause 52.215-1, Offerors are responsible for submitting proposals, and any modifications or revisions, so as to reach the Government office designated in the Solicitation by the time specified in the Solicitation. FAR clause 52.215-1, Instructions to Offerors – Competitive Acquisition (Jan 2004) is hereby incorporated in this Pre-Solicitation by reference.

7.0 Research Topics

7.1 S&T Directorate Topic

The following are the topics for the FY23 S&T Directorate's SBIR Program:

DHS231-001 - Accurate and Real-time Hardware-assisted Detection of Cyber Attacks

DHS231-002 - Air Cargo Manifest Analysis to Aid Screeners

DHS231-003 - First Responder Digital Badges

DHS231-004 - Machine Learning Based Integration of Alarm Resolution Sensors

DHS231-005 - Mission Critical Services Server-to-Server Communication, voice communications, 3GPP-Standards

DHS231-006 - Reduced Order Modeling of Critical Infrastructure Protect Surfaces

7.2 CWMD Office Topics

The following are the topics for the FY23 CWMD SBIR Program:

DHS231-007 - Theoretical Classification Methodologies to Enable Detection with Predicted Signatures

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

APPENDIX A – RESEARCH TOPIC DESCRIPTIONS

SBIR Topic Number: DHS231-001

TITLE: Accurate and Real-time Hardware-assisted Detection of Cyber Attacks

TECHNOLOGY AREAS: Sensors, Cybersecurity, Electronics, Artificial Intelligence, Internet of Things (IoT)

OBJECTIVE: Develop a hardware-assisted real-time accurate detector of cyber-attacks on networked and edge electronic devices.

DESCRIPTION: An increasing number of network-connected devices and systems in modern-day life are vulnerable to many attacks. Beyond the traditional computing systems and cloud services, modern Internet-of-Things (IoT) and cyber-physical systems can experience numerous cyber-attacks, such as ransomware, spyware, spoofing, botnets, keyloggers, denial of service (DoS), and distributed denial of service (DDoS), each of which is becoming more prevailing by numbers, as well as more challenging to thwart. There is an on-going need for effective solutions to identify, report and protect against cyber-threats. Current protection techniques are limited in detection efficacy (~70%) and scalability issues. Most techniques are primarily based-upon static software-focused solutions such as code analysis and signature (template) matching. These techniques have proven to be limited in detection efficacy so far, as reflected by the increasing number of threats and compromised cases.

This topic is seeking solutions to analyze hardware generated data that would enable real-time, precise detection (>95%) and proactive protection against cyber-threats. The end state of this effort is a device-embedded solution to support highly accurate, real-time (within fraction of seconds) detection of critical cyber-threats, such as crypto-ransomware and DDoS attacks, on networked and edge electronic devices, such as computers, servers, cyber-physical systems, and IoT devices with minimal performance overhead while offering multi-layer and distributed defense, monitoring anomalous behaviors against zero-day attacks, and engaging automatic protection without human intervention.

PHASE I: Determine the technical feasibility of accurate (>85% detection efficacy), real-time, and automatic detection of cyber threats using hardware-assisted modalities that includes:

1) Determination of the major challenges and preliminary assessment of machine learning algorithms for extracting features of various cyber-threats
2) Development of an initial concept model considering hardware features and emerging approaches in machine learning for anomaly detection.

PHASE II: Based on the concept model developed in Phase I, develop and demonstrate a prototype for real-time and automatic detection of cyber-threats. The prototype deliverables would include:

1) Establishment of a performance parameter through experimental analysis of the critical hardware-assisted features to cover a wide variety of cyber threats
2) Design and development of the automatic hardware-assisted threat sensing and artificial intelligence algorithms to demonstrate high confidence in detecting cyber-threats in compromised devices
3) Define in-field runtime monitoring and detection objectives, device-embedded architecture, and demonstration of efficacy for rapid detection of cyber threats.
4) A technical roadmap that takes the program through Phase III should be part of the final delivery for Phase II.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: Highly efficient, real-time, automatic device-embedded detection for prevailing cyber threats, such as ransomware and DDoS, have the potential to benefit both government and commercial operations for protecting critical assets, preventing unauthorized access to data, and maintaining a secure and live network for critical applications.

Refine the developed algorithms and trained models of the automatic detection system prototype solution for in-field application under commercial or government usage by testing against a large pool of cyber threats. Success metrics include the versatility of protected electronic devices, ease of use for advanced and legacy systems, high detection confidence (>99%), and performance/cost overhead of the device if any.

REFERENCES:

1. McAfee Labs Threats Report, June 2021 - https://www.mcafee.com/enterprise/en-us/assets/reports/rp-threats-jun-2021.pdf
2. Crowdstrike 2022 Global Threat Report - https://www.crowdstrike.com/global-threat-report/
3. Tehranipoor, Mark, University of Florida (2021). *Emerging Topics in Hardware Security*. Gainesville, FL: Springer

KEY WORDS: Hardware-assisted security; DDoS; Cybersecurity; Machine learning; Feature extraction; Malware; Ransomware.

TECHNICAL POINT OF CONTACT:

Michael Vichich, michael.vichich@hq.dhs.gov

SBIR Topic Number DHS231-002

TITLE: Air Cargo Manifest Analysis to Aid Screeners

TECHNOLOGY AREAS: Baggage, Cargo, People Screening

OBJECTIVE: Develop software to correlate items on a shipping manifest with images obtained from the screening of air cargo skids.

DESCRIPTION: Air cargo screening is performed by Transportation Security Administration (TSA) regulated entities. As private enterprises these entities need to screen air cargo for aviation security threats in an effective manner but also need to do so in economically viable ways.

Screening air cargo through whole-skid X-ray Computed Tomography (CT) Explosive Detection Systems (EDS) imaging is a challenging enterprise. Air cargo skids are an approximate maximum size of 48" x 65" x 48", which is much larger than checked baggage items, and contain much more diverse items ranging from fresh produce, to medicines, to dense electronics and heavy machine parts. Screeners are frequently called upon to break down skids and screen items individually (through X-ray, explosive trace detection and/or physical search) when X-ray images are not definitive enough to determine that no threats are contained within. This leads to increased costs in staffing requirements and decreased throughput.

X-ray systems used to screen air cargo skids can distinguish organic, inorganic and metallic items for the screeners. Air cargo manifests are a source of information of what the skids contain and could be used to inform screeners of what to expect in an X-ray image. Air cargo manifest information could also be used to inform a screener when items are present that are sufficiently dense, cluttered or known to scatter X-rays (such as books or pallets of water) are and likely to present difficulties in X-ray screening.

Software that can serve to decrease the number of skids that must be broken down for individual examination, resulting in increasing efficiency and saving costs for the regulated entity as well as ensuring improved screening and threat interdiction.

The proposed solution should present high-level analytic conclusions to a screener based on the air cargo manifest. It should also allow screeners to call up the air cargo manifest and work in concert with existing X-ray and future CT-based (EDS) air cargo skid screening systems. It is envisioned that this solution would be standalone with a connection (e.g. an ethernet or USB interface to a standard PC) to the screening system and not integrated into existing devices

PHASE I: Design and develop an innovative detailed proof of concept, to the level of pseudo code, for processing air cargo manifests, identifying data to highlight for the security screener and correlate them with the skid being screened.

PHASE II: Develop and demonstrate a software prototype that graphically provides information relating the air cargo manifest to skid images that enables screeners to identify specific cargo items and any potential challenges in screening a skid through X-ray/CT (EDS) images. Deliverables would include technical reports describing how the software operates (including how it interfaces with the screening system) and how it was validated.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: The homeland security applications of potential development would include interface to X-ray (including CT) and EDS based screening systems at a TSA regulated entity. The technology could possibly be adapted to other homeland security enterprises.

REFERENCES:

1. Snapshot: S&T Funds Solution to Increase Efficiency of Air Cargo Screening - https://www.dhs.gov/science-and-technology/news/2019/03/05/snapshot-st-looks-increase-air-cargo-screening-efficiency
2. TSA Cargo Programs - https://www.tsa.gov/for-industry/cargo-screening-program
3. Air Cargo Security: TSA Field Testing Should Ensure Screening Systems Meet Detection Standards - https://www.gao.gov/products/gao-21-105192

KEY WORDS: Air cargo screening; Language processing; X-ray; CT; Manifest; TSA; Software; EDS.

TECHNICAL POINT OF CONTACT:

Kumar Babu, kumar.babu@hq.dhs.gov

SBIR Topic Number DHS231-003

TITLE: First Responder Digital Badges

TECHNOLOGY AREAS: Cybersecurity, Communications & Digital Trust

OBJECTIVE: Develop an interoperable digital software badge capability that can securely and efficiently prove a first responder personnel's identity and qualifications onsite in a disaster response operating environment.

DESCRIPTION: Many first responder organizations at various levels, inclusive of government, local and state, and non-profit agencies each have different methods on identifying first responders on scene during an incident. The lack of an interoperable and standardized credentialing solution for first responders results in more challenges with communication and coordinated access to information, such as the coordination of personnel and for residents and victims who may need transportation, medical assistance, food and shelter, etc.

The current emergency response involves first responders arriving in-person at the scene, communicating via mobile land radio and networked digital applications. Current credentialing solutions like plastic identity badges, such as Personal Identity Verification (PIV), and Personal Identity Verification-Interoperable (PIV-I), are costly at approximately $132 and generally not integrated with field applications and platforms. Moreover, PIV-based badge solutions are not easily extended to support additional attributes or integrate with resource management applications and logistics in a dynamic environment. Paper printed credentials that are simple to manufacture (such as printed vaccination cards) are easily counterfeited and are not strongly verifiable. Other approaches are more resistant to counterfeiting but use proprietary encodings that in turn are not universally readable. These solutions cannot continue to be effectively and safely utilized as many incidents are dangerous to operate in, have legal protections (crime scene), or un-approved personnel may interfere with or thwart responders' actions in furtherance of their own agenda or plan (criminal acts/terrorism). A new capability is required to make large scale incident and events safer for the public and responders by ensuring only authorized personnel are allowed to work inside the emergency area. A more flexible suite of credentials and universal verification is needed for our response community to respond to incidents securely and efficiently.

New international standards, including the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) 18013-5, and ISO/IEC 23220 series are being adopted by some state and Federal government organizations in the U.S., and by the private sector and internationally, for credentialing citizens. Credentialing encompasses proof of identity, including verification and validation of name, age, home and work addresses, employment, etc. on and offline without needing to connect back to the issuing organization. The format (mdoc) is extensible to other types of credentials including first responders. Several large phone equipment manufacturers (Google, Samsung, Apple) in 2022 and other emerging technology companies are rolling out digital wallets, along with consuming U.S state issued driving licenses and identification cards. An additional standard, Decentralized Identifiers (DIDs) v1.0 is emerging as an alternative for verifiable digital identity credentialing.

The proposed solution should adhere to these defined standards, and should include the following

requirements:

- Credentials must include:
  - Name
  - Title
  - Organization
  - Jurisdiction
  - Qualifications

Qualifications should include credentials that prove the individual has an array of skills that have been verified against the Federal Emergency Management Agency (FEMA) National Incident Management System (NIMS) guidelines.

- Credentialing information should be able to be shared and communicated online and offline to other first responders prior to allowing access to the site or venue.
- Ability to be tracked and monitored, dynamically over a wide range of emergency operational situations and via a wide range of network conditions, inclusive of high latency, degradation of network bandwidth and broadcast ability, and no network ability.
- Ability to send verified identification information in a secure packet to the specific authorized receiver collecting the credentials. It should occur in real time, with a validation or authorization process that is cryptographic hardware based.
- Should not require specialized hardware to issue, hold or be verified. Can be used with existing first responder hardware that first responders already have available, (smart phone, laptop, smartwatch, etc.) that has trusted execution environments.
- The digital identity credential information should be sent and received in a standardized format easily accessed and understood by authorized users of the system that is interoperable and doesn't require proprietary software protocols to be issued, held or verified.

PHASE I: Design and develop an innovative proof of concept for how a First Responder agency could credential their employees/members via a smartphone or other online compatible device to be received and accessed by another smart device or online service. This phase will validate the process roles, hardware, software, and criteria involved in provisioning identity credentials and reading the credential from another device or service to another. Critical cross organizational functions, such as situational awareness and command and control, etc. shall be included in the feasibility study.

PHASE II: Building on the information from Phase I, the technology demonstration should prove interoperability across devices and/or services to allow for in-person validation of credential, online verification of credential and the ability for it to function in a communications constrained environment (lack of or intermittent cellular or other communications method). Selected scenarios used during the demonstration should highlight and quantify any solution constraints resulting from materials, processes, and equipment, such as overall durability of the solution during multiple users accessing at the same time, and any human factors that may impede the solution from functions.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: The potential for first responder credentialing for the Homeland Security Enterprise (HSE) is the ability to use the credentialing capability as the foundation for resource management during emergency response, multi-agency coordination utilizing the secure resource identification and authentication into DHS platforms. This application could also increase security of

information sharing through the Homeland Security Information Network (HSIN) and other multi-agency platforms that have varying requirements e.g. (sworn law enforcement only) and provide better on-line access solutions than username and password that are susceptible to breaches and phishing. This can benefit SLTT partners, FEMA, USSS and HSI where task forces or other multi-agency use cases apply.

The commercial applications for this solution are multi-faceted and can include badge replacement, time keeping improvement, improved system security access for vendors who sell into the first responder space. As vehicles increasingly become computers with wheels the replacement of car keys, other physical access tokens where logs/permissions for access to systems, facilities or vehicles could benefit from the development of this technology. Building on the wave of innovation occurring off the underlying standards and rapid improvement in smartphones the commercial application market is expected to grow quickly. This capability ensures the Government will not be stuck with supporting outdated, non-interoperable, poor usability solutions that can come from public sector only solutions.

REFERENCES:

1. INCIDENT MANAGEMENT SYSTEM Guideline for the National Qualification System https://www.fema.gov/sites/default/files/2020-05/fema_nims_nqs_guideline_0.pdf
2. ISO/IEC 18013-5:2021 Personal identification — ISO-compliant driving license — Part 5: Mobile driving license (mDL) application https://www.iso.org/standard/69084.html
3. Cards and security devices for personal identification — Building blocks for identity management via mobile devices — Part 1: Generic system architectures of mobile eID systems https://www.iso.org/standard/74910.html
4. Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations. https://www.w3.org/TR/did-core/
5. Verifiable Credentials Data Model v1.1. https://www.w3.org/TR/vc-data-model/

KEY WORDS: Identity; Credentialing; First-responder; Authentication; Interoperability; Public key infrastructure (PKI); Privacy preserving.

TECHNICAL POINT OF CONTACT:

Karen Johnson, karen.johnson@hq.dhs.gov

SBIR Topic Number DHS231-004

TITLE: Machine Learning Based Integration of Alarm Resolution Sensors

TECHNOLOGY AREAS: Explosives Alarm Resolution (AR) at Aviation Checkpoints and Security Checkpoints.

OBJECTIVE: Develop an integrated Alarm Resolution sensor suite with smart algorithms to enable high collection efficiency of explosive samples and signatures and enhance AR detectors' performance, while simultaneously reducing user information overload.

DESCRIPTION:
Explosive threats come in all shapes, sizes, concealments, and nuanced formulations. Due to these complexities, DHS Components employ a variety of detectors from Explosives Trace Detectors (ETD) based on both Ion Mobility Spectrometry and Mass Spectrometry, vapor detectors, bulk resolution detection (Infrared (IR) and Raman based), through barrier detection (Spatially Offset Raman Spectrometry), and colorimetric kits. However, having a multitude of AR tools can lead to information overload in end-users.

Information overload is especially pronounced in crowded and high throughput environments such as aviation and security checkpoints. As a baseline, a Transportation Security Officer (TSO) currently would have to follow a multi-step decision tree to screen and resolve an alarm of a suspicious object. As part of this, the TSO would have to characterize shapes, sizes, and color of objects and to mentally categorize objects according to their utilities and compositions. From these initial screenings, they would determine the best tool(s) at their disposal to detect and identify explosives whether it is an ETD, colorimetric, IR, Raman, vapor detector, or any combination thereof. They would then determine how best to sample and collect explosives signatures whether it is through swabbing residues at frequently touched surfaces or aiming a laser to excite unknown substances and collecting their signatures.

One way to reduce information overload is through rigorous training. TSOs are trained on how to execute the decision tree and with practices of sampling techniques, they develop muscle memory (i.e. with the use of a Pressure Sensitive Wand). However, such training could only alleviate information overload incrementally. Thus, one alarmed object after another and day after day, TSOs may experience a high level of information overload which accumulates over time leading to user fatigue.

In response to this topic, S&T seeks a proposed solution to develop a new capability that comprehensively alleviates aforementioned information overload on the users. This capability would characterize shapes, sizes, and color of objects and from this initial characterization, categorize objects according to their utilities and compositions. From these initial screenings, the capability would inform a user on the best tool(s) to detect and identify explosives. The proposed capability solution should consist of three sub-components, all integrated within a desktop size box:
1) New sensors which can scan the object and categorize material compositions according to their physical characteristics (ex: electrical conductivity, magnetic property...);
2) A Machine Learning algorithm that takes sensory output, analyzes, and suggests the best AR detector to sample or collect signatures of unknown substances; and
3) Upon user confirmation, actuate the AR detector to detect and identify explosives.

This is in essence a decision analytics tool specifically applied toward enhanced Alarm Resolution.

Performance parameters for this proposed capability include the Probability of Categorizing (PC) correctly objects according to their utilities and function (Phases 1 and 2) and the Probability of Recommending (PR) the right AR tool(s) (Phase 3). For comparison, PC and PR will be collected from a well-informed TSO who employs the AR decision tree according to five different bins of characteristics and functions and four different AR tools.

PHASE I: In Phase I, the Offeror will demonstrate feasibility of proposed approach of sensors to generate sensory outputs and from/through these outputs, the task of characterization of objects can be achieved. Objects are characterized according to their:

1) Shapes, sizes and colors;
2) Utilities (ex: books, clothes, bottles, packages, electronics...);
3) Compositions (paper, glass, plastics, metals...);
4) Whether there are fingerprints on the outside of the object; and
5) Whether there are gas, liquid, and or solid inside the object.

For this demonstration, no algorithms are needed in this phase.

PHASE II: The Offeror will demonstrate a Machine Learning based algorithm which can fully characterize an object based on sensory outputs developed in Phase I. The solution must include training/learning, validation, and test and evaluation phases as well as types of training/learning either supervised or unsupervised. In the training/learning process, a dataset will be developed consisting of:

- Stream of commerce objects commonly seen at aviation checkpoints such as clothing articles, books, bottles, pouches, electronics, and objects with coverings,
- At least five classes of materials (ex: paper, glass, plastics, metals, wood, and cotton), and
- Having sufficient sample sizes to generate statistically significant results.

Deliverables for Phase II includes two prototypes consisting of sensors integrated into a box with dimensions no larger than 22 inches (length); 24 inches (height); and 22 inches (width). The perception algorithm will be integrated into these prototypes. The prototypes will communicate to the users via voice and a graphic user interface on PC and PR results. The two prototypes will demonstrate their ability to correctly categorize (PC) objects according to their utilities.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: In Phase III, the Offeror will further incorporate Alarm Resolution sensors into the two prototypes. AR sensors consist of ETD sensors, vapor detector, Raman Spectroscopy-based detectors, and standoff detectors. Based on these AR sensors, the updated system will be further trained, validated, and tested and evaluated on their probability of recommending (PR) the right AR tool(s). A key requirement of Phase III is the ability of the integrated system to automatically actuate the right AR tool to detect and identify explosives. The actuation of AR sensor(s) has to be done in such a way that it:

1. Enhance the collection of explosive signatures by collecting samples/signatures at optimal locations and by applying optimal pressures to surfaces of an object under investigation,
2. Collect samples/signatures using multiple AR sensors either concurrently or in sequence, and
3. Actuation of one sensor does not impede the functions of others.

The Government will communicate to the Offeror specific AR sensors to be used in this Phase. For each AR tool, there is a detection requirements document. Such integrated solutions will enhance detection capabilities of Homeland Security Enterprise (HSE) end users.

Although applications of this Machine Learning based decision analytics tool initially focus on helping HSE end users, such decision analytics tool could be modified and applied widely in scenarios involving local law enforcement and/or first responders. For example, police officers responding to a potential drug overdose may have to make a decision on whether to administer naloxone or to collect opioid samples for prosecution. This decision analytics tool could characterize surfaces and surrounding environments on whether there are trace residues of opioids and from there help guide the officers on the best course of action. The ultimate goal is to employ integrated technologies to minimize information overload and to increase first responders' ability to focus on their mission.

REFERENCES:

1. Nevatia, Ramakant, 1982, Machine Perception, Englewood Cliffs, NJ: Prentice-Hall.
2. Thoi Nguyen and Laura Parker, Trace Explosives Detection Workshop, 2022, New Orleans, LA, (Integration of Alarm Resolution Sensors).
3. ALERT COE ADSA Conference of 2011, Awareness and Localization of Explosives-Related Threats Center of Excellence, Algorithm Development for Security Applications. The whole workshop involved discussion of sensor fusions, https://alert.northeastern.edu/transitioning-technology/adsa/

KEY WORDS: Machine Learning; Machine Perception; Algorithms; Alarm Resolution; Capabilities; Sensor Integration.

TECHNICAL POINT OF CONTACT:

Dr. Thoi Nguyen, thoi.nguyen@hq.dhs.gov

SBIR Topic Number DHS231-005

TITLE: Mission Critical Services Server-to-Server Communication, voice communications, 3GPP-Standards

TECHNOLOGY AREAS: First Responder, Conformance, Interoperability, Mission Critical Services, 3GPP, Interworking Function (IWF), Compatibility

OBJECTIVE: Develop testing methods and processes to ensure conformance and interoperability of Mission Critical Services server-to-server communications.

DESCRIPTION: Mission critical services were implemented in the Third Generation Partnership Project (3GPP) standards to provide public safety users with highly resilient and high-performance network capabilities, such as quality of service, priority and preemption.

Cellular network providers are starting to provide Mission Critical Services (MCS or MCX) to their customers in the form of Mission Critical Push To Talk (MCPTT), Mission Critical Video (MCVideo), and Mission Critical Data (MCData). However, communications and interoperability among users on different carriers, or on different vendor furnished applications, can be limiting. MCS services consist of both end point applications on user equipment and the servers that provision and manage those services. Though MCS servers exist within a cellular network provider's core network, there are other devices that can act as a MCS server. An example of this is portable dispatcher units that a customer may use.

Since these services are relatively new, the interfaces between the servers and their implementation are not mature and are likely to be non-interoperable and not conform to the standards. Furthermore, there exists proprietary technology that could hamper communications and interoperability. (Non-interoperable solutions will be a barrier to interoperability between public safety users using different services). The National Institute of Standards and Technology's (NIST) Public Safety Communications Research Division (PSCR) has recently funded grants to perform MCS device and application conformance test cases. Currently, there is no test equipment that can perform server conformance test cases. And there is no unified process and methodology to conduct interoperability testing for MCS server-to-server communications.

The 3GPP has created server-to-server conformance test cases in the document TS 36.579-3 for MCPTT, but it has no plans to create conformance test tools for these test cases. There are 3GPP work plans to greatly expand the scope of the document to include server aspects for MCVideo and MCData, in addition to expanding the number of test cases for MCPTT. (e.g., TTCN-3). This effort will build upon the NIST PSCR effort to build test tools to enable conformance and interoperability testing between MCS servers of different cellular network providers. This solution will develop testing equipment to test server conformance and a process & methodology for testing interoperability to insure that first responders maintain communications during critical incidents and planned events per the standard(s) [see references]. This is especially needed if the users are trying to communicate while using multiple cellular network providers or solution providers.

PHASE I: Develop the process for executing the conformance test cases found in 3GPP TS 36.579-3 and define the feasibility of creating the test equipment to conduct these test cases. Analysis should present how this tool and process can be validated, used and tested. Proposals should define how once developed; this (these) Tool(s) can be enhanced in the future to address emerging MCX standards from 3GPP. The tool should enable testing both locally and remotely. It is expected that the tool will be used both domestically and internationally.

A requirements matrix should be established to define a conformance test suite from the available test cases in 3GPP TS 36.579-3 to conduct the performance, conformance and interoperability testing including MCS server-to-server communications.

PHASE II: The process to execute the conformance test cases found in 3GPP TS 36.579-3, and the test equipment to execute the test cases, will be prototyped and demonstrated. Documentation should provide traceability between the specified standards and the testing capability. As required, the solution will be tested and updated with representative solutions. Also, the process and methodology to test server-to-server interoperability will be prototyped and demonstrated.

Demonstration and test should be designed in such a manner as to validate the requirements matrices produced in Phase I.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: Development and deployment of the MCS server-to-server testing will be critical to maintaining interoperable communications for first responders. Commercialization could take a variety of forms. Five possible realizations include, but are not limited to:

1. Customer owned/maintained test equipment that can execute MCS server-to-server conformance test cases. The test equipment can be sold to interested parties.

2. Customer owned/maintained test facility that utilizes the MCS server-to-server conformance test equipment and associated processes to provide testing services for interested parties.

3. Customer owned/maintained test facility that utilizes the process and methodology to test MCS server-to-server interoperability to provide testing services for interested parties.

4. Customer owned/maintained test facility that provides both MCS server-to-server conformance and interoperability testing services.

5. Software as a Service to conduct remote testing of implementation

REFERENCES:

1. 3GPP TS 36.579-1 "Mission Critical (MC) services over LTE; Part 1: Common test environment"; https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3155
2. 3GPP TS 36.579-2 "Mission Critical (MC) services over LTE; Part 2: Mission Critical Push To Talk (MCPTT) User Equipment (UE) Protocol conformance specification";

https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3156

3. 3GPP TS 36.79-3 "Mission Critical (MC) services over LTE; Part 3: Mission Critical Push To Talk (MCPTT) Server Application conformance specification"; https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3157
4. 3GPP TS 36.579-4 "Mission Critical (MC) services over LTE; Part 4: Test Applicability and Implementation Conformance Statement (ICS) proforma specification"; https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3158
5. 3GPP TS 36.579-5 "Mission Critical (MC) services over LTE; Part 5: Abstract test suite (ATS)"; https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3159
6. 3GPP TS 36.579-6 "Mission Critical (MC) services over LTE; Part 6: Mission Critical Video (MCVideo) User Equipment (UE) Protocol conformance specification"; https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3463
7. 3GPP TS 36.579-7 "Mission Critical (MC) services over LTE; Part 7: Mission Critical Data (MCData) User Equipment (UE) Protocol conformance specification"; https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3464
8. 3GPP TS 23.280 "Common functional architecture to support mission critical services"; https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3086

KEY WORDS: MCPTT; MCVideo; MCData; 3GPP; MCS; MCX; MCX-1; Push-to-Talk; PTT.

TECHNICAL POINT OF CONTACT:
Russell Becker, russell.becker@hq.dhs.gov

SBIR Topic Number DHS231-006

TITLE: Reduced Order Modeling of Critical Infrastructure Protect Surfaces

TECHNOLOGY AREAS: Critical Infrastructure, Advanced Computing, Network Modeling, Cybersecurity Research

OBJECTIVE: Develop a technique for generating reduced-order models of the protect surface of a cyber-physical-human critical infrastructure system enabling a comprehensive vulnerability assessment against catastrophic, model-based destabilization attacks.

DESCRIPTION: Today's critical infrastructures are complex, dynamic, cyber-physical-human systems. These systems often can hide intricate sensitivities to small perturbations that can result in catastrophic, destabilizing behaviors, such as cascading failures in a power grid or a stock market's flash crash. Enemies with enough information about the system can exploit these sensitivities and design provably stealthy attacks to trigger them, so detecting the presence of these sensitivities, or these intrinsic vulnerabilities, is the first step towards protecting our critical infrastructure systems from this next-generation of sophisticated model-based attacks.

Many such model-based attacks in critical infrastructure systems are beginning to emerge [1]. For example, machine learning can be used to design catastrophic attacks in a number of systems, such as in chemical processing plants, power generation or distribution systems, heating, ventilation, and air conditioning (HVAC) systems, water treatment or distribution systems, or nuclear power facilities. A general model may be known- from basic physics, but where specific parameters for a particular target facility are learned through stealthy observation of that system's behavior. Nevertheless, even though details about designing and executing such attacks are increasingly available in the academic literature, little work has been done developing techniques to systematically detect and protect against them. Guaranteed robustness analyses [2] provide one approach to secure these systems, but the nonlinear and often hybrid nature of these systems, and their sheer complexity, make performing such computations extremely difficult at scale.

The protect surface of the critical infrastructure is a model that represents system variables that are hypothesized as being potentially exposed to possible attackers (or other unexpected perturbations), as well as their causal relationships to each other; dynamical structure functions have been used to build such models for linear time invariant systems. When building these models, choosing which variables are "exposed", and which variables are suppressed as part of the causal interaction between exposed variables, allows modelers to distinguish insider attacks, where many more system variables may be exposed, from other attacks where fewer variables may be exposed. Nevertheless, the number of exposed variables and the complexity of the, often nonlinear, dynamics can make these models unwieldy and impractical to develop for real critical infrastructure systems.

New research is needed to develop methodologies for reduced-order modeling of the protect surfaces for critical infrastructure systems, such as power systems, chemical and other manufacturing facilities, municipal and regional water systems, nuclear reactors, emergency services, transportation networks, pipelines, commercial and government facilities, financial

systems, dams, communication networks, or food production and agricultural systems. These reduced order models should preserve critical properties of the full system, such as stability and sensitivity to perturbations of the exposed variables, while significantly reducing the complexity of the model. The reduced order model should exhibit the same vulnerability properties as the full model so that a comprehensive vulnerability analysis conducted on the reduced model will reveal the vulnerabilities and exploitation potential of the actual system. For more information on approaches for developing such reduced order models might be found in [3] and related works. A proposed solution should provide an approach to building the reduced models of a system, that can maintain the vulnerability properties of that system. It will provide an exemplar for the process, and a tool(s) to assist others in developing such models.

PHASE I: Prove feasibility of proposed methodology for a simplified model of a system's protect surface that preserves vulnerability properties of the original model. Demonstrate the viability of this methodology on a specific critical infrastructure system as an area of focus and build a simulation model (i.e. the “full system model”) of least one exemplar system from that focus area. So, for example, if power systems were chosen as the area of focus, then the IEEE 39-Bus System is one exemplar system that could be chosen for the Phase I study. The exemplar system should be representative for the infrastructure under investigation, be non-trivial, and be well-documented, preferably from the relevant academic or professional literature, with a complete mathematical description of its physical behavior.

PHASE II: Develop a prototype code base to implement the model simplification methodology. This code base should be well architected with the potential for being the foundational code base for commercial activities without significant refactoring. Demonstrate code on a model of an organization that manages and controls a critical infrastructure that would be found in a targeted area.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: Homeland Security Applications focus on developing new sophisticated tools capable of conducting the necessary computations, at scale, to detect vulnerabilities of critical infrastructures to novel model-based attacks. These attacks may use machine learning to learn specific model parameters for infrastructure systems, such as a particular chemical processes plant or a particular city's municipal water system. The computation necessary to detect vulnerability to such attacks can be intractable, so the model-reduction methodology developed in this effort could be necessary to protect these infrastructures against such attacks. Although it is not clear that the same methodology will work for all critical infrastructure systems, as these systems exhibit very different dynamics, it seems very likely that methodologies should be available at least for infrastructure systems that are well described by physical models, such as power, water, nuclear, and chemical manufacturing systems, etc. The Cybersecurity and Infrastructure Security Agency (CISA) should certainly be one component served by this technology, but, depending on the critical infrastructure studied, Transportation Security Agency (TSA) or other components might also benefit.

REFERENCES:

1. H. E. Brown and C. L. Demarco, "Risk of Cyber-Physical Attack via Load With Emulated Inertia Control," in *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 5854-5866, Nov. 2018.

2. Zhou, K., & Doyle, J. C. (1998). Essentials of robust control (Vol. 104). Upper Saddle

River, NJ: Prentice Hall.

3. Machta, Benjamin B., et al. "Parameter space compression underlies emergent theories and predictive models." *Science* 342.6158 (2013): 604-607.

KEY WORDS: Reduced-order modeling; Critical infrastructure resilience; Protect surface; Model-based attacks; Vulnerability analysis; Cyber-physical-human security.

TECHNICAL POINT OF CONTACT:

Brent Talbot, brent.talbot@hq.dhs.gov

CWMD Topic Number: DHS231-007

TITLE: Theoretical Classification Methodologies to Enable Detection with Predicted Signatures

TECHNOLOGY AREAS: Chemical Detection, Chemical Computations, Algorithms

OBJECTIVE: Classification software that derives theoretically calculated signatures/spectra of unknown, not yet created, toxic compounds.

DESCRIPTION: The government seeks innovative methods to create theoretical spectroscopic signatures of potentially toxic chemical compounds for use in detection systems. Compounds of interest include chemical warfare agents (CWAs), toxic industrial compounds (TICs), pharmaceutical based agents (PBAs), and non-traditional agents (NTAs). Compounds of interest could be naturally occurring or synthetic. Novel classification, identification, and quantification methods can provide enormous savings in cost and timelines for fielding new detector systems and can improve the reliability and performance of both current and future systems. These enhancements will ultimately result in increased safety for the public and Department of Homeland Security operational units when encountering novel agents.

Detection systems that rely on target materials' spectroscopic signatures have been limited to the detection, and possible quantification, of known compounds whose signatures have been measured experimentally. This project will introduce the ability to expand libraries of spectroscopic signatures beyond that limited set by (1) the automated generation of molecular structures, (2) theoretical prediction of their spectroscopic signatures, and (3) predictions of their toxicity metrics. This will dramatically expand the range of potentially toxic materials that may be detected, even with existing detection systems. Present technologies for spectrum prediction include the use of molecular dynamics to simulate single molecules and clusters of molecules, and density functional theory (DFT); some employ machine learning algorithms. However, these techniques still lack sufficient accuracy to fill the needs of the Department of Homeland Security.

The project entails developing theoretical spectra of toxic compounds, such as CWAs, TICs, PBAs, NTAs, and similar compounds. The work could proceed from low molecular weight to higher molecular weight compounds. Algorithms for classification may focus on a chosen spectroscopic technology and to provide tools to enable theoretically based identification. This effort is meant to develop algorithms; the choice of platform (e.g. cloud or edge computing) is up to the performer. Estimation of toxicity metrics of chemicals in the above-listed classes, including as-yet unknown threat agents, can be defined by immediately dangerous to life and health (IDLH) metrics following NIOSH/OSHA standards. Finally, data formats must be non-proprietary. Standard data formatting will enable efficient data processing and reachback analysis.

PHASE I: Establish the technical feasibility of employing predicted signatures, rather than experimentally obtained results, for classification of materials using current chemical detection technologies including, but not limited to, electrochemical, optical spectroscopies (Ultraviolet–visible/Infrared/Raman), Liquid Chromatography (LC), Gas Chromatography (GC), Mass Spectrometry (MS), and Nuclear Magnetic Resonance (NMR). Provide a plan for the practical development and integration of the proposed signature prediction techniques as a component of an operational detection system. The final report shall detail modeling/simulation methods for discovery of novel toxic threat compounds and estimation of their physical properties and toxicity.

The ability to develop system performance metrics for complex threat agents needs to be demonstrated in Phase I.

PHASE II: Finalize development of the algorithm and experimental proof-of-concept testing and validation using test simulants that have not been previously observed by the software. This could involve derivative chemical simulant materials other than that of training data used in Phase I. Phase II implements the simulated data analytics efforts into a proof-of-concept demonstration of the algorithm's functionality in a lab environment. The software shall provide confidence metrics for toxicity and predicted spectral features. Finally, to ensure broader community use of the software, performers will be encouraged to work with the Government and industry to create a data format standard.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS
Theoretical algorithms that can be integrated into technical reachback capabilities in addition to current and/or next generation operational detector technologies to enable the detection of as-yet unknown threats. Detection technologies that could benefit from the proposed effort include various levels of resolution, from handheld field deployable units to benchtop analytical grade instruments. As such the capability developed should have functionality included to allow cross platform modifications to align with native resolution of instrumentation. The offeror could also develop a theoretical signature software platform for existing instruments to save research resources.

REFERENCES:
1. Gastegger. M., Behler. J., & Marquetand. P. (2017). *Machine Learning Molecular Dynamics for the Simulation of Infrared Spectra*. Chem. Sci, 8, 6924 -6935. https://doi.org/10.1039/C7SC02267K.
2. Ye. S., Zhong. K., Zhang. J., Hu. W., Hirst. J. D., Zhang. G., Mukamel. S., & Jiang. J. (2020). *A Machine Learning Protocol for Predicting Protein Infrared Spectra*. J. Am. Chem. Soc*, 142*(45), 19071 -19077. https://doi.org/10.1021/jacs.0c06530.
3. Wang. Y., Yang. F., Wu. P., Bu. D., & Sun. S. (2015). *OpenMS-Simulator: An Open-Source Software for Theoretical Tandem Mass Spectrum Prediction*. BMC Bioinformatics, *16*, 110. https://doi.org/10.1186/s12859-015-0540-1.
4. Vosegaard. T. (2018). *Fast Simulations of Multidimensional NMR Spectra of Proteins and Peptides*. Magnetic Resonance in Chemistry, *56*(6), 438 -448. https://doi.org/10.1002/mrc.4663.
5. Urbina F, Lowden CT, Culberson JC, & Ekins S. (2022) *MegaSyn: Integrating Generative Molecular Design, Automated Analog Designer, and Synthetic Viability Prediction.* ACS Omega *7*(22), 18699-18713. https://doi: 10.1021/acsomega.2c01404.

KEY WORDS: Chemical, Threats, Detection, Identification, Test, Computational Discrimination

TECHNICAL POINT OF CONTACT:
CWMD R&D Division, CWMD.SBIR@hq.dhs.gov
Eric Riffle, eric.riffle@hq.dhs.gov

APPENDIX B – DEFINITIONS

Commercialization. The processes of developing products, processes, technologies, or services and the production and delivery (whether by the originating party or others) of products, processes, technologies, or services for sale to or use by the Federal Government or commercial markets.

Conflicts of Interest. Contract awards made to small business concerns owned by or employing current or previous Federal Government employees could create conflicts of interest for those employees, which may be a violation of federal law of FAR Part 3.601 and the Ethics in Government Act of 1978, as amended. Small business Concerns that are owned by or employ current or previous Federal Government employees should seek guidance from the cognizant Ethics Counselor from the employee's Government agency.

Essentially Equivalent Work. Work that is substantially the same research, which is proposed for funding in more than one contract proposal or grant application submitted to the same Federal agency or submitted to two or more different Federal agencies for review and funding consideration; or work where a specific research objective and the research design for accomplishing an objective are the same or closely related to another proposal or award, regardless of the funding source.

Foreign National (Foreign Person). A foreign national (foreign person) means any person who is not:

a) A citizen or national of the United States; or
b) A lawful permanent resident; or
c) A protected individual as defined by 8 U.S.C. 1324b(a)(3).

"Lawful permanent resident" is a person having the status of having been lawfully accorded the privilege of residing permanently in the United States as an immigrant in accordance with the immigration laws and such status not having changed.

"Protected individual" is an alien who is lawfully admitted for permanent residence, is granted the status of an alien lawfully admitted for temporary residence under 8 U.S.C. 1160(a) or 8 U.S.C. 1255a(a)1, is admitted as a refugee under 8 U.S.C. 1157, or is granted asylum under 8 U.S.C. 1158; but does not include (i) an alien who fails to apply for naturalization within six months of the date the alien first becomes eligible (by virtue of period of lawful permanent residence) to apply for naturalization or, if later, within six months after November 6, 1986, and (ii) an alien who has applied on a timely basis, but has not been naturalized as a citizen within two (2) years after the date of the application, unless the alien can establish that the alien is actively pursuing naturalization, except that time consumed in the Service's processing the application shall not be counted toward the 2-year period.

False Statements. Knowingly and willfully making any false, fictitious, or fraudulent statements or representations, may be a felony under the False Statement Act (18 U.S.C. § 1001), punishable by a fine of up to $10,000, up to five years in prison, or both.

Fraud, Waste and Abuse.
Fraud – Includes any false representations about a material fact or any intentional deception designed to deprive the United States unlawfully of something of value or to secure from the United States a benefit, privilege, allowance, or consideration to which an individual or business is not entitled.
Waste – Includes extravagant, careless or needless expenditure of Government funds, or the consumption of Government property, that results from deficient practices, systems, controls, or decisions.
Abuse – Includes any intentional or improper use of Government resources, such as misuse of rank, position, or authority or resources.

Funding Agreement. Any contract, or grant, or cooperative agreement entered into between any Federal Agency and any small business concern for the performance of experimental, developmental, or research work, including products or services, funded in whole or in part by the Federal Government.

Joint Venture. See 13 CFR 121.103(h).

Key Individual (Key Personnel). The principal investigator/project manager and any other person named as a "key" employee in a proposal submitted in response to the 23.1 Solicitation.

Principal Investigator/Project Manager. The one individual designated by the Offeror to provide the scientific and technical direction to a project supported by the funding agreement.

Proprietary Information. Proprietary information is information that is provided which constitutes a trade secret, proprietary commercial or financial information, confidential personal information or data affecting the national security.

Research or Research and Development (R/R&D). Any activity that is:
a) A systematic, intensive study directed toward greater knowledge or understanding of the subject studies;
b) A systematic study directed specifically toward applying new knowledge to meet a recognized need; or
c) A systematic application of knowledge toward the production of useful materials, devices, and systems or methods, including design, development, and improvement of prototypes and new processes to meet specific requirements.

Research Involving Animal Subjects. DHS has adopted the principles of the U.S. Department of Agriculture (USDA) implementation of the Animal Welfare Act, the Public Health Service (PHS) implementation of the Health Care extension Act, and the other related federal principles and guidelines as they represent the ethical foundation for the care and use of animals in research. All research involving the care and use of animals in research shall be conducted in accordance with DHS Management Directive Number 026-01.

Research Involving Human Subjects. DHS has adopted Department of Health and Human Services (HHS) policies governing human subjects research, as set forth in 45 C.F.R. Part 46 (Subparts A-

D). Subpart A of 45 C.F.R. part 46 is HHS' codification of the Federal Policy for the Protection of Human Subjects (also known as The Common Rule) which represents the basic foundation for the protection of human subjects in most research conduct or supported by U.S. Federal departments and agencies. All research involving human subjects shall be conducted in accordance with DHS Management Directive Number 026-04.

SAFETY Act. Congress enacted the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (the "SAFETY Act") as part of the Homeland Security Act of 2002. The SAFETY Act provides limitations on the potential liability of those concerns that develop and provide qualified anti-terrorism technologies. The DHS Science and Technology Directorate, acting through its Office of SAFETY Act Implementation, encourages the development and deployment of anti-terrorism technologies by making available the SAFETY Act's system of "risk management" and "liability management."

Offerors submitting proposals in response to the 23.1 Solicitation are encouraged to submit SAFETY Act applications on their applicable existing technologies/products and are invited to contact the Office of SAFETY Act Implementation (OSAI) for more information at 1-866-788-9318 or visit OSAI's website at www.safetyact.gov.

SBIR Technical Data. All data generated during the performance of an SBIR award.

SBIR Technical Data Rights. The rights an SBIR awardee obtains in data generated during the performance of any SBIR Phase I, Phase II, or Phase III award that an awardee delivers to the Government during or upon completion of a Federally funded project, and to which the Government receives a license. See FAR 52.227-20.

Small Business Concern. A concern that meets the requirements set forth in 13 C.F.R. 121.702.

State Assistance. Many states have established programs to provide services to those small business concerns and individuals wishing to participate in the Federal SBIR Program. These services vary from state to state, but may include:

- Information and technical assistance.
- Matching funds to SBIR recipients; and/or
- Assistance in obtaining Phase III funding.
  Visit https://www2.ed.gov/programs/sbir/state_awards.html for further information.

Subcontract. Any agreement, other than one involving an employer-employee relationship, entered into by an awardee of a funding agreement calling for supplies or services for the performance of the original funding agreement. This includes consultants.

ATTACHMENT 1: SBIR FUNDING CERTIFICATION – TIME OF AWARD

All small businesses that are selected for award of an SBIR/STTR Funding Agreement must complete this certification at the time of award and any other time set forth in the Funding Agreement that is prior to performance of work under this award. This includes checking all of the boxes and having an authorized officer of the Awardee sign and date the certification each time it is requested.

Please read carefully the following certification statements. The Federal Government relies on the information to determine whether the business is eligible for a Small Business Innovation Research (SBIR) program or Small Business Technology Transfer (STTR) program award. A similar certification will be used to ensure continued compliance with specific program requirements during the life of the Funding Agreement. The definitions for the terms used in this certification are set forth in the Small Business Act, SBA regulations (13 CFR part 121), the SBIR/STTR Policy Directive and also any statutory and regulatory provisions referenced in those authorities.

If the Funding Agreement officer believes that the business may not meet certain eligibility requirements at the time of award, they are required to file a size protest with the U.S. Small Business Administration (SBA), which will determine eligibility. At that time, SBA will request further clarification and supporting documentation in order to assist in the verification of any of the information provided as part of a protest. If the Funding Agreement officer believes, after award, that the business is not meeting certain Funding Agreement requirements, the agency may request further clarification and supporting documentation in order to assist in the verification of any of the information provided.

Even if correct information has been included in other materials submitted to the Federal Government, any action taken with respect to this certification does not affect the Government's right to pursue criminal, civil or administrative remedies for incorrect or incomplete information given in the certification. Each person signing this certification may be prosecuted if they have provided false information.

The undersigned has reviewed, verified and certifies that (all boxes must be checked unless otherwise directed):

(1) ☐ The Awardee business concern meets the ownership and control requirements set forth in 13 CFR 121.702.

(2) If a corporation – all corporate documents (namely: articles of incorporation and any amendments, articles of conversion, by-laws and amendments, shareholder meeting minutes showing director elections, shareholder meeting minutes showing officer elections, organizational meeting minutes, all issued stock certificates, stock ledger, buy-sell agreements, stock transfer agreements, voting agreements, and documents relating to stock options, including the right to convert non-voting stock or debentures into voting stock) must evidence that the corporation meets the ownership and control requirements set forth in 13 CFR 121.702. (Check one box).

☐ Yes ☐ N/A Explain why N/A:

(3) If a partnership -- the partnership agreement evidences that it meets the ownership and control requirements set forth in 13 CFR 121.702. (Check one box).

☐ Yes ☐N/A Explain why N/A:

(4) If a limited liability company – the articles of organization and any amendments, and operating agreement and amendments, evidence that it meets the ownership and control requirements set forth in 13 CFR 121.702. (Check one box).

□ Yes □ N/A Explain why N/A:

(5) The birth certificates, naturalization papers, or passports show that any individuals it relies upon to meet the eligibility requirements are U.S. citizens or permanent resident aliens in the United States. (Check one box).

□ Yes □ N/A Explain why N/A:

(6) □ The Awardee business concern has no more than 500 employees, including the employees of its Affiliates.

(7) □ SBA has not issued a size determination currently in effect finding that this business concern exceeds the 500 employee size standard.

(8) During the performance of the award, the Principal Investigator/Project Manager will spend more than one half of his/her time (based on a 40 hour workweek) as an employee of the Awardee (or Research Institution – STTR only) or has requested and received a written deviation from this requirement from the Funding Agreement officer. (Check one box).

□ Yes □ Deviation approved in writing by Funding Agreement officer: _%

(9) All Essentially Equivalent Work, or a portion of the work, proposed under this project (check applicable line):

□ **Has not** been submitted for funding to this Agency or another Federal agency.

□ **Has** been submitted for funding to this Agency or another Federal agency **but has not** been funded under any other grant, contract, subcontract or other transaction.

□ A portion has been funded by another grant, contract, or subcontract as described in detail in the proposal and approved in writing by the Funding Agreement officer.

(10) During performance of award, the Awardee will perform the applicable percentage of work unless a deviation from this requirement is approved in writing by the Funding Agreement officer (check applicable line and fill in if needed):

□ SBIR Phase I: at least two-thirds (66 2/3%) of the research.

□ SBIR Phase II: at least half (50%) of the research.

STTR Phase I or Phase II: at least forty percent (40%) of the research.

□ Deviation approved in writing by the Funding Agreement officer (SBIR only): __%

(11) During performance of award, the R/R&D will be performed in the United States unless a deviation is approved in writing by the Funding Agreement officer (check one box).

□ Yes □ Waiver has been granted

(12) □ During performance of award, the R/R&D will be performed at the Awardee's facilities by the Awardee's employees, except as otherwise indicated in the SBIR/STTR application and approved in the Funding Agreement.

(13) The SBIR Awardee has registered itself on SBA's database as majority-owned by venture capital operating companies, hedge funds or private equity firms (check one box).

□ Yes □ No □ N/A Explain why N/A: _____

(14) The SBIR Awardee is a Covered Small Business Concern (a Small Business Concern that: (a) was not majority-owned by multiple venture capital operating companies (VCOCs), hedge funds, or private equity firms on the date on which it submitted an application in response to an SBIR solicitation; and (b) on the date of the SBIR award, which is made more than 9 months after the closing date of the solicitation, is majority-owned by multiple venture capital operating companies, hedge funds, or private equity firms). (Check one box).

□Yes □No

(15) □ I will notify this Agency immediately if all or a portion of the work authorized and funded under this award is subsequently funded by another Federal Agency.

(16) [*For STTR only*] The Small Business Concern, and not a partnering Research Institution, is exercising management direction and control of the performance of the STTR Funding Agreement.

□Yes □No

(17) □ I understand that the information submitted may be given to Federal, State, and local agencies for determining violations of law and other purposes.

(18) □ I am an officer of the business concern authorized to represent it and sign this certification on its behalf. By signing this certification, I am representing on my own behalf, and on behalf of the business concern that the information provided in this certification, the application, and all other information submitted in connection with this application, is true and correct as of the date of submission. I acknowledge that any intentional or negligent misrepresentation of the information contained in this certification may result in criminal, civil or administrative sanctions, including but not limited to: (1) fines, restitution and/or imprisonment under 18 U.S.C. 1001; (2) treble damages and civil penalties under the False Claims Act (31 U.S.C. 3729 et seq.); (3) double damages and civil penalties under the Program Fraud Civil Remedies Act (31 U.S.C. 3801 et seq.); (4) civil recovery of award funds, (5) suspension and/or debarment from all Federal procurement and nonprocurement transactions (FAR subpart 9.4 or 2 CFR part 180); and (6) other administrative penalties including termination of SBIR/STTR awards.

Signature	*Date_/_/___*
Print Name (First, Middle, Last)	
Title	
Business Name	

ATTACHMENT 2: SBIR FUNDING CERTIFICATION – LIFE CYCLE CERTIFICATION

All SBIR/STTR Phase I and Phase II Awardees must complete this certification at all times set forth in the Funding Agreement (see § 8(j) of the SBIR/STTR Policy Directive). This includes checking all of the boxes (unless otherwise directed) and having an authorized officer of the Awardee sign and date the certification each time it is requested.

Please read carefully the following certification statements. The Federal Government relies on the information to ensure compliance with specific program requirements during the life of the Funding Agreement. The definitions for the terms used in this certification are set forth in the Small Business Act, the SBIR/STTR Policy Directive, and also any statutory and regulatory provisions referenced in those authorities.

If the Funding Agreement officer believes that the business is not meeting certain Funding Agreement requirements, the agency may request further clarification and supporting documentation in order to assist in the verification of any of the information provided.
Even if correct information has been included in other materials submitted to the Federal Government, any action taken with respect to this certification does not affect the Government's right to pursue criminal, civil or administrative remedies for incorrect or incomplete information given in the certification. Each person signing this certification may be prosecuted if they have provided false information.
The undersigned has reviewed, verified and certifies that (all boxes must be checked except where otherwise directed):

(1) The Principal Investigator/Project Manager spent more than one half of his/her time (based on a 40 hour workweek) as an employee of the Awardee (or Research Institution – STTR only) or the Awardee has requested and received a written deviation from this requirement from the Funding Agreement officer.

□ Yes □ No □ Deviation approved in writing by Funding Agreement officer: %

(2) All Essentially Equivalent Work, or a portion of the work, performed under this project (check the applicable line):

□ **Has not** been submitted for funding to this Agency or another Federal Agency.

□ **Has** been submitted for funding to this Agency or another Federal agency **but has not** been funded under any other grant, contract, subcontract or other transaction.

□ A portion has been funded by another grant, contract, or subcontract as described in detail in the proposal and approved in writing by the Funding Agreement officer.

(3) Upon completion of the award, the Awardee will have performed the applicable percentage of work, unless a deviation from this requirement is approved in writing by the Funding Agreement officer (check the applicable line and fill in if needed):

□ SBIR Phase I: at least two-thirds (66 2/3%) of the research.

□ SBIR Phase II: at least half (50%) of the research.

□ Deviation approved in writing by the Funding Agreement officer (SBIR only): __%

(4) The work is completed, and the small business Awardee has performed the applicable percentage of work, unless a deviation from this requirement is approved in writing by the Funding Agreement officer (check the applicable line and fill in if needed):

- □ SBIR Phase I: at least two-thirds (66 2/3%) of the research.
- □ SBIR Phase II: at least half (50%) of the research.
- □ Deviation approved in writing by the Funding Agreement officer: __%
- □ N/A because work is not completed

(5) The R/R&D is performed in the United States unless a deviation is approved in writing by the Funding Agreement officer.

□Yes □No □Waiver has been granted

(6) The R/R&D is performed at the Awardee's facilities by the Awardee's employees, except as otherwise indicated in the SBIR/STTR application and approved in the Funding Agreement.

□Yes □No

(7) □ I will notify this Agency immediately if all or a portion of the work authorized and funded under this award is subsequently funded by another Federal Agency.

(8) □ I understand that the information submitted may be given to Federal, State, and local agencies for determining violations of law and other purposes.

(9) □ I am an officer of the Awardee business concern authorized to represent it and sign this certification on its behalf. By signing this certification, I am representing on my own behalf, and on behalf of the business concern, that the information provided in this certification, the application, and all other information submitted in connection with the award, is true and correct as of the date of submission. I acknowledge that any intentional or negligent misrepresentation of the information contained in this certification may result in criminal, civil or administrative sanctions, including but not limited to: (1) fines, restitution and/or imprisonment under 18 U.S.C. 1001; (2) treble damages and civil penalties under the False Claims Act (31 U.S.C. 3729 et seq.); (3) double damages and civil penalties under the Program Fraud Civil Remedies Act (31 U.S.C. 3801 et seq.); (4) civil recovery of award funds, (5) suspension and/or debarment from all Federal procurement and non-procurement transactions (FAR subpart 9.4 or 2 CFR part 180); and (6) other administrative penalties including termination of SBIR/STTR awards.

Signature	*Date_/_/___*
Print Name (First, Middle, Last)	
Title	
Business Name	

ATTACHMENT 3: BRIEFING CHART TEMPLATE

<table>
<tr><td colspan="2"><u>Proposal Title Company City, State</u>
<u>Proposal Number:</u></td></tr>
<tr><td>Place a clear photograph, drawing, graphic or diagram of the concept related to innovation here

Provide a simple, legible, but sufficiently detailed graphic to convey the main concept or idea of the research effort and/or development prototype.</td><td><u>Relevance and Goals and Commercialization</u>

Relevance and Goals:
Research goals and desired end state including performance targets
Advantages over other state-of-the-art solutions
Key technical challenges

Commercialization Strategy:
Describe the current market potential for product/service development and estimated unit cost of the product
Identify end user interests or agreements</td></tr>
<tr><td><u>Technical Objectives and Work Plan</u> Address:
Technological innovations supporting the approach, as appropriate
How the problem will be addressed
The current status of the proposed effort
The key technical challenges and/or risks
The planned technical accomplishments/key milestones

<u>Estimate the Technology Readiness Level (TRL 1 – 9) at beginning and end of contract</u></td><td><u>Milestones, Deliverables, Schedule and Team</u>

Milestones, Deliverables and Schedule:
Provide milestones, primary deliverables, and task durations for Phase I and Phase II, as appropriate

Team:
List the proposing organization and principal investigator
List subcontractors</td></tr>
<tr><td colspan="2">NON-PROPRIETARY, UNCLASSIFIED DATA</td></tr>
</table>

ATTACHMENT 4: CWMD NON-DISCLOSURE AGREEMENT

NON-DISCLOSURE AGREEMENT
TOPIC SOLICITATION <Insert Topic Solicitation Number>

The Parties to this Agreement agree that Mayvin Inc. and its supporting consultants and subcontractors also under non-disclosure agreement, may have access to proprietary information of Offeror contained within the technical and cost proposals, solely to perform technical advisory services for the Government, in evaluating proposals submitted in response to this Solicitation.

The Parties agree to protect the proprietary information from unauthorized use or disclosure for as long as it remains proprietary, and to refrain from using the information for any purpose other than that for which it was furnished.

_____
Company Name (Offeror)

_____
Name of Company Official (Offeror), Printed

_____ _____
Signed Dated

_____
Pat McGovern
Mayvin, Inc.

_____ _____
Signed Dated

ATTACHMENT 5: Solicitation Provisions and Contract Clauses

This Solicitation incorporates one or more provisions or clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a provision or clause may be accessed electronically at http://acquisition.gov/comp/far/index.html.

Federal Acquisition Regulation (48 CFR Chapter 1) Provisions/Clauses Incorporated by Reference:

52.202-1	Definitions	JUN 2020
52.203-3	Gratuities	APR 1984
52.203-5	Covenant Against Contingent Fees	MAY 2014
52.203-6	Restrictions on Subcontractor Sales to the Government	JUN 2020
52.203-7	Anti-Kickback Procedures	JUN 2020
52.203-8	Cancellation, Rescission and Recovery of Funds for Illegal or Improper Activities	MAY 2014
52.203-10	Price or Fee Adjustment for Illegal or Improper Activity	MAY 2014
52.203-11	Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions	JUN 2020
52.203-12	Limitation on Payments to Influence Certain Federal Transactions	OCT 2010
52.203-17	Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights	APR 2014
52.204-1	Approval of Contract	DEC 1989
52.204-4	Printed or Copied Double-Sided on Postconsumer Fiber Content Paper	MAY 2011
52.204-7	System for Award Management	OCT 2018
52.204-14	Service Contract Reporting Requirement	OCT 2016
52.204-19	Incorporation by Reference of Representation and Certifications	DEC 2014
52.204-21	Basic Safeguarding of Contractor Covered Information	JUN 2016
52.204-24	Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment	OCT 2020
52.204-25	Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment	AUG 2020
52.209-2	Prohibition on Contracting with Inverted Domestic Corporations-Representation	NOV 2015
52.209-5	Certification Regarding Responsibility Matters	AUG 2020
52.209-6	Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment	OCT 2015
52.209-7	Information Regarding Responsibility Matters	OCT 2018
52.209-9	Updates of Publicly Available Information Regarding Responsibility Matters	OCT 2018
52.209-10	Prohibition on Contracting with Inverted Domestic Corporations	NOV 2015
52.215-2	Audits	
52.215-8	Order of Precedence – Uniform Contract Format	OCT 1997
52-215-10	Price Reduction for Defective Cost or Pricing Data	AUG 2011
52.215-12	Subcontract Cost or Pricing Data	OCT 2010
52.215-13	Restriction on Certain Foreign Purchase	JUN 2008
52.215-20	Requirements for Cost or Pricing Data Information Other Than Cost or Pricing Data	OCT 2010
52.216-1	Type of Contract	APR 2014
52.219-1	Small Business Program Representations	NOV 2020
52.219-8	Utilization of Small Business Concerns	OCT 2018

52.219-14	Limitations on Subcontracting	JAN 2017
52.222-3	Convict Labor	JUNE 2003
52.222-21	Prohibition of Segregated Facilities	APR 2015
52.222-26	Equal Opportunity	SEP 2016
52.222-35	Equal Opportunity for Veterans	JUN 2020
52.222-36	Equal Opportunity for Workers with Disabilities	JUN 2020
52.222-37	Employment reports on Veterans	JUN 2020
52.222-50	Combating Trafficking in Persons	OCT 2020
52.222-54	Employment Eligibility Verification	OCT 2015
52.223-18	Encouraging Contractor Policies to Ban Text Messaging While Driving	JUN 2020
52.227-11	Patent Rights-Ownership by the Contractor	MAY 2014
52.227-20	Rights in Data-SBIR Program	MAY 2014
52.232-2	Payments under Fixed-Price Research and Development Contracts	APR 1984

Federal Acquisition Regulation (48 CFR Chapter 1) Provisions/Clauses Incorporated by full text:

52.204-23 PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES (DEVIATION 20-05)

(a) Definitions. As used in this clause-
"Covered article" means any hardware, software, or service that-
(1) Is developed or provided by a covered entity;
(2) Includes any hardware, software, or service developed or provided in whole or in part by a covered entity; or
(3) Contains components using any hardware or software developed in whole or in part by a covered entity.
"Covered entity" means-
(1) Kaspersky Lab;
(2) Any successor entity to Kaspersky Lab;
(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or
(4)Any entity of which Kaspersky Lab has a majority ownership.
(b) Prohibition. Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub.
L. 115-91) prohibits Government use of any covered article. The Contractor is prohibited from-
(1) Providing any covered article that the Government will use on or after October 1, 2018; and
(2) Using any covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.
(c) Reporting requirement.
(1) In the event the Contractor identifies covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report, in writing, via email, to the Contracting Officer, Contracting Officer's Representative, and the Enterprise Security Operations Center (SOC) at NDAA Incidents@hq.dhs.gov, with required information in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Enterprise SOC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.
(2) The Contractor shall report the following information pursuant to paragraph (c)(1) of this clause:
(i) Within 1 business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the report pursuant to paragraph (c)(l) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.
(d) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts, including subcontracts for the acquisition of commercial items.
(End of clause)

52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (DEVIATION 20-05) (AUG 2020)

(a) Definitions. As used in this clause—
"Backhaul" means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).
"Covered foreign country" means The People's Republic of China.
"Covered telecommunications equipment or services" means–
(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);
(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or
(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.
"Critical technology" means–
(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;
(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-
(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or
(ii) For reasons relating to regional stability or surreptitious listening;
(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);
(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);
(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or
(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).
"Interconnection arrangements" means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g.,

connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.
"Reasonable inquiry" means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.
"Roaming" means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.
"Substantial or essential component" means any component necessary for the proper function or performance of a piece of equipment, system, or service.
(b) Prohibition.
(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115–232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.
(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115–232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.
(c) Exceptions. This clause does not prohibit contractors from providing—
(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or
(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.
(d) Reporting requirement.
(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause in writing via email to the Contracting Officer, Contracting Officer's Representative, and the Enterprise Security Operations Center (SOC) at NDAA_Incidents@hq.dhs.gov, with required information in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Enterprise SOC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.
(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause
(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.
(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.
(End of clause)

52.204-26 Covered Telecommunications Equipment or Services-Representation (Oct 2020)

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause
(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(a) *Definitions.* As used in this provision, "covered telecommunications equipment or services" and "reasonable inquiry" have the meaning provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) *Procedures.* The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (https://www.sam.gov) for entities excluded from receiving federal awards for "covered telecommunications equipment or services".

(c)

(1) *Representation.* The Offeror represents that it does, ___does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(2) After conducting a reasonable inquiry for purposes of this representation, the offeror represents that it □ does, □ does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services.