Department of Homeland Security

Phase 0 Program for New SBIR Applicants

How a Small Business can Approach Understanding the FY25.1 DHS SBIR Phase I Pre-Solicitation

PRESENTED BY

Jenny C. Servo, Ph.D.

Agenda

- Download the PPT and Pre-solicitation

- The DHS SBIR program

- What is a Pre-Solicitation?

- Contracting vs Granting organizations

- What is unique about the Pre-Solicitation?

- How is the Pre-solicitation organized

- Review the 5 Topics and correspond with TPOCs

- Period of Performance for Phase I and $ Ceiling

- SAM application for companies that are new to federal contracting

- The Phase 0 program for the Department of Homeland Security

DHS Small Business Innovation Research (SBIR)

- There are 11 agencies that offer the Small Business Innovation Research (SBIR) program and five that have a Small Business Technology Transfer (STTR) program

- The Department of Homeland Security (DHS) has an SBIR program ONLY

- DHS has one solicitation per year, usually released in the November timeframe

- DHS topics come from two organizations within DHS: **the Science & Technology (S&T) office** and the **Countering Weapons of Mass Destruction (CWMD) office**

- This is a competitive process. Proposals are evaluated based on
  - Technical merit
  - Staff qualifications and capability
  - Potential for commercialization
  - Cost/price

Contracting vs Granting Organizations

- Some of the participating agencies make their awards as grants and some as contracts

- Granting organizations include DOE, NSF, USDA, NOAA, NIST, HHS

- Contracting organizations included DoD, DHS, NASA, DOT, EPA

- Grants are made to accomplish a public purpose and the agency is typically NOT a customer for the resulting goods and services

- Contracting organizations procure goods and services that will directly benefit the government

- Contracts and grants follow different rules – one relates to if and when you can talk to topic authors

4

What is a Pre-Solicitation?

- When the federal government is the intended customer, the agency goes through a process to assure that what the Topics are clear and that they have time to conduct outreach

- The DHS 25.1 Phase I SBIR Pre-Solicitation was released on **November 13, 2024** and is provided for planning purposes through December 11th

- This will be followed by the DHS 24.1 Phase I SBIR Solicitation on **December 17, 2024**

- Phase I proposals can be submitted between **December 17, 2024 and January 21, 2025**

- It is possible that there may be some differences between the Pre-Solicitation and the Solicitation

5

What is unique about the Pre-Solicitation?

- The Pre-Solicitation lists the topic authors, commonly referred to as Technical Points of Contact (TPOCs)

- Their contact information is listed at the bottom of each of the five FY25.1 DHS SBIR topics

- You can reach out to them during the Pre-solicitation period via email to ask questions of clarification

- Once the pre-solicitation period closes on December 11th, you can no longer reach out to them personally

- However, you can pose questions for public response on January 6, 2025

- Q&A posted on SAM.gov, January 10, 2025

How is the Pre-Solicitation organized?

- The Pre-solicitation contains many detailed guidelines and is a resource for planning

- It also contains two Appendices and Three Attachments

- Your starting point should be Appendix A which contains the five topic descriptions and the Technical Point of Contacts e-mail addresses

- You need to review the Topics and determine if you can submit a proposal that addresses the specified needs

Sample Topic DHS251-004

SBIR Topic Number: DHS251-004

TITLE: Securing Video Communications to Prevent Digital Injection Attacks

TECHNOLOGY AREAS: Trusted Digital Identity, Remote Identity Verification and Cybersecurity

OBJECTIVE: Develop innovative software that can secure multiparty video interactions and defeat known digital injection attacks.

DESCRIPTION: The Department of Homeland Security (DHS) is seeking software that can establish and maintain digital trust in video being captured by a camera in a laptop, desktop, or mobile device while connected with video conferencing applications. DHS requires this technology to support operational goals such as conducting virtual interviews for immigration beneficiaries. DHS is increasingly doing business online including immigration interviews, remote identity proofing and agency meetings online. The ability to transact digitally with trust is key to multiple DHS missions. Widely used video platforms such as Microsoft Teams, Zoom, Webex, etc., allow substitution of virtual cameras with no notice or awareness to the participants in a video interaction. This deficiency can allow for video injection attacks.

Current research solutions focus on passive detection techniques based on verification of received imagery, and other solutions incorporate active measures based on particular hardware [5]. An example of current solutions is Presentation Attack Detection (PAD), an automated determination of the presentation attack. Although there has been progress, not all approaches can be integrated for real-time streaming video, and few detectors are robust over various methods of generating live deepfakes (content modification) on all commodity personal computers. The dynamically changing and rapidly improving methods for generating live deepfakes may defeat some detectors, resulting in an ongoing challenge between generators and detectors. This topic is seeking an innovative solution to mitigate and prevent digital injection attacks where a bad actor could modify live video content to deceive, commit fraud, or perpetrate scams.

The proposed solution should:
1. Establish and maintain integrity of the video stream between two or more commodity laptops or other consumer hardware, such as desktops and mobile devices.
2. Indicate to both users the system is secure and notify user if there is any security change during the video interaction.
3. Integrate with existing operating systems, drivers, hardware and video applications.
4. Demonstrate novel and distinct capability from existing commercial presentation attack detection solutions and liveness detection solutions.
5. Be interoperable and use open standards where at all possible.
6. Solution should be immune from digital injection attacks as defined at a minimum in CEN/TC 224.

PHASE I: Determine the viability of the proposed solution's computer security approaches to prevent digital injection attacks by establishing, maintaining and communicating digital trust. Determine what capabilities and/or extended functions are needed by video applications and where those functions would need to reside across operating systems, device drivers, application software, and camera hardware. The performer must explain how the proposed solution integrates with existing operating systems, drivers, hardware, and video applications and how the proposed solution is novel and distinct from existing commercial presentation attack detection solutions.

PHASE II: Develop a prototype of the proposed solution, that will provide a detailed model of software security layers necessary for a video application to alert participants that the video or imagery data is originating from a real camera and that the video content has not been modified. The solution prototype will provide the necessary

security utilities to verify and assert there is a secure channel between a video application and a personal computer camera.

PHASE III: COMMERCIAL OR GOVERNMENT APPLICATIONS: Phase III has cross cutting potential applications for homeland security applications that perform remote identity verifications and all video conferencing applications. Secure video channels using commodity hardware will potentially benefit the homeland security enterprise, as well as commercial business communications. Phase III may include adoption and integration into applications that require trusted video using commodity hardware such as immigration interviews, remote identity proofing transactions for disaster assistance, video communications between DHS personnel and other government use cases. Phase III will include user interface options for video applications to indicate "trusted video" sources, providing a visual indication to trust the interaction (e.g., lock icon for https in a browser, checkmark for a verified account, etc.).

REFERENCES:
1. News Release: DHS S&T Announces Track 3 of the Remote Identity Validation Tech Demo Challenge. https://www.dhs.gov/science-and-technology/news/2024/01/23/dhs-st-announces-track-3-remote-identity-validation-tech-demo-challenge
2. Biometric Authentication Under Threat: Liveness Detection Hacking. https://i.blackhat.com/USA-19/Wednesday/us-19-Chen-Biometric-Authentication-Under-Threat-Liveness-Detection-Hacking.pdf
3. Video injection attacks: What is that and the way forward? https://www.biometricupdate.com/202405/video-injection-attacks-what-is-that-and-the-way-forward
4. Finance worker pays out $25 million after video call with deepfake 'chief financial officer'. https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk
5. Digital Identity Guidelines: Identity Proofing and Enrollment. https://csrc.nist.gov/pubs/sp/800/63/a/4/2pd
6. StandICT.eu. CEN/TC Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment. https://2020.standict.eu/standards-watch/centc-224-personal-identification-and-related-personal-devices-secure-element

KEYWORDS: digital injection attack rebroadcasting video real-time deepfake generation

TECHNICAL POINT OF CONTACT:
Jonathan Prisby
jonathan.prisby@hq.dhs.gov

What Types of Questions can you ask?

- "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."

- Be sure to carefully read all the information provided first and the references, before you prepare an email to send to the TPOC
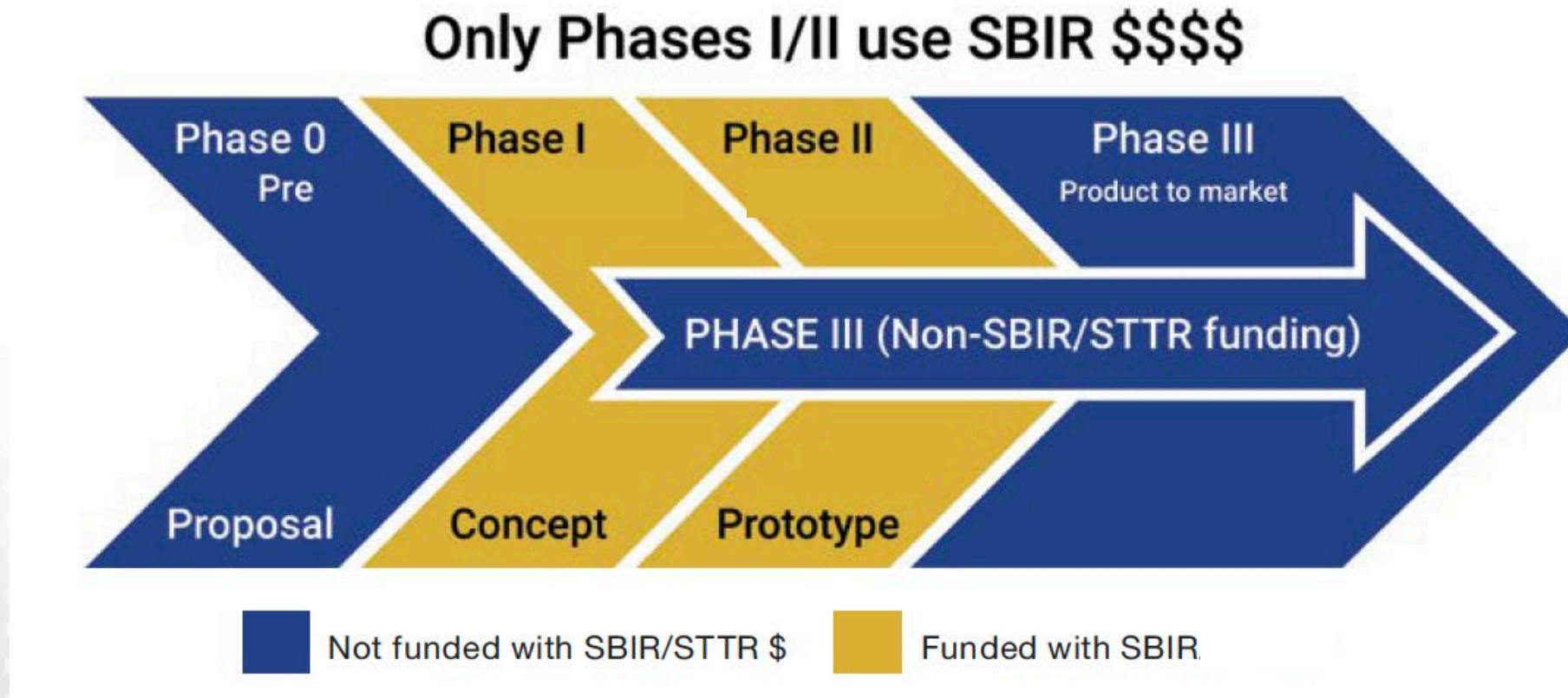
Other important items in Pre-Solicitation

SBIR Topic Proposal Structure*

Phase I	Phase II
$175,000**	$1,000,000 - $1,500,000***
5 months	24 months – 36 months

Proposal Structure may be modified in 25.1 Solicitation or in Phase II Proposal Submission Instructions. Phase II Proposal Submission Instructions will provide specific maximum funding threshold.

How Does the SBIR PROGRAM WORK?

Only Phases I/II use SBIR $$$$

Phase 0 Pre — Proposal
Phase I — Concept
Phase II — Prototype
Phase III Product to market
PHASE III (Non-SBIR/STTR funding)

Not funded with SBIR/STTR $ Funded with SBIR

Why is the SBIR Program Beneficial for Small Business?

You receive funding to conduct R&D with no strings attached

- You don't give up equity
- It is <u>NOT</u> a loan
- You own the intellectual property

Who is Eligible to Submit a DHS SBIR Proposal?

- Must be a for profit, small business at the time of award
- A small business is defined as a company with less than 500 employees
- The company must be primarily U.S. owned – defined as 51% of its ownership being by U.S. citizens or permanent resident aliens,
- R&D must be performed by the applicant and subcontractors in the U.S.
- Small businesses that are majority owned by multiple venture capital firms, hedge funds or private equity firms are not eligible
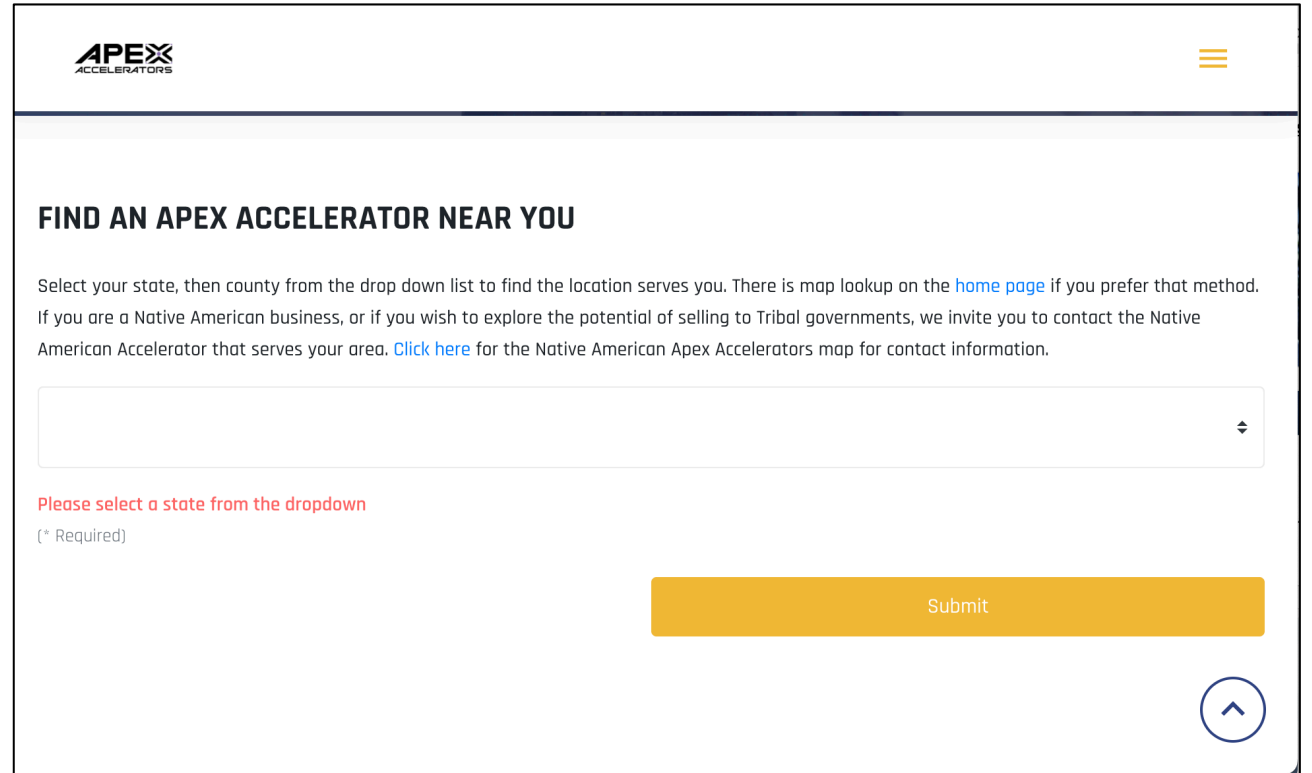
What Registrations are Required?

- SAM Registration
  - This is time consuming and should be started now. Use the APEX ACCELERATORS
  - Unique Entity ID (UEI) – created as part of SAM registration process
  - Commercial and Government Entry (CAGE) code – created as part of SAM registration process
  - SAM registration 3 to 4 weeks to secure. Important to start right away
  - If you are not registered with SAM you cannot submit a proposal
- SBA Company Registration Database

Important Registration – SAM System for Awards Management

- This registration is required in order to submit a proposal to any agency

- The SAM registration process has multiple steps, over time as the system verifies information with other systems

- Important to start this process right away

- Contact APEX Accelerators

- https://www.apexaccelerators.us/#/

What are the Key Elements of the <u>Proposal</u>?

	Mandatory Proposal Requirements	Phase I
System Generated	Cover Sheet	As generated by the system
	Briefing Chart	As generated by the system
	Cost Proposal	As generated by the system
	Project Plan	As generated by the system
	Foreign Access Management Screening Form 11055	As generated by the system – if applicable
	Disclosure of Foreign Affiliations	As generated by the system
PDF Upload	Technical Proposal	Limited to 15 Pages
	SBA Company Registration	Limited to 1 Page
	Commercialization Report	N/A

See Page 6 of FY25.1Pre-Solicitation

The Technical Proposal is the <u>Most Important!</u>

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

More detailed guidelines start on Page 8 of the Pre-Solicitation

Content First, Format Second

- Single column format

- 12-point Times New Roman with 1" margins

- Company name, topic number and proposal number must be included in header on every page

- 10-point font is permissible for embedded tables, figures, graphics and Table of Contents (if included)

- Perform a virus check before uploading

What Does Non-responsive Mean?

- The term NON-RESPONSIVE means that the company did not submit all the required parts of the proposal and therefore, the materials submitted will NOT BE REVIEWED
- You will be categorized as NON-REPONSIVE if,
  - You did not upload a copy of the SBA Registration
  - You exceeded the maximum cost or the period of performance
  - Failed to include the Disclosure of Foreign Relationships form
  - Did not include all mandatory sections and exceeded the page limits

Phase 0 SBIR Program

For the Department of Homeland Security

A MULTI-TIER PROCESS

Webinar Series
Always 2:00 – 3:00 EST

How a Small Business Should Approach Understanding the Pre-Solicitation	November 21
Confirming Eligibility and Using your Time Wisely	November 26
How to Prepare your Technical Proposal	December 3
Principal Investigators and Other Personnel	December 5
Preparing your Budget	December10
Protecting Your Intellectual Property	December 12
Important Forms to Submit with your DHS proposal	December 17
DHS SBIR Proposal Submission Process	December 19
Looking Ahead: Setting Up a Government Accounting System	January 7, 2025

22

Proposal Preparation Mentoring Service

- Option for those new to proposal prep process
- For the mentoring service, there is a more detailed application
- We review the application to assure the company has an approach for addressing the topic
- We then contact service providers in your area to find one who can provide mentoring assistance to you
- We will check in with you to see how things are going

Thank-you for joining us today!

- Sign up for the webinar series
- If you have never written a proposal before and would like to receive mentoring assistance, please complete the registration form
- Please take a moment to provide your feedback on today's webinar

- See the website for [Phase 0 SBIR program for DHS!](#)

Please take a moment to complete a very short Feedback form

https://forms.office.com/r/L8BD6BRgV4