Assessing Security of Encrypted Messaging Applications (ASEMA)
HR0011SB20254-12
Frequently Asked Questions (FAQs)

https://www.darpa.mil/research/programs/asema

As of 24 September 2025

Q1. Does ASEMA expect the use of XAI/ML for vulnerability detection, or is the emphasis on traditional cryptographic analysis?

A1. The ASEMA SBIR expects the security risks of the applications themselves, more specifically the code that interacts with the network and the mobile operating system, to be assessed. Cryptographic protocols used by secure messaging applications (SMAs) are already well-understood and well-tested security properties, and therefore not the focus of this effort.

Q2. Are there priority operational contexts (e.g., tactical units, coalition partners) for this capability?

A2. There are no priority operational contexts for this capability.

Q3. Will performance be judged more on detection accuracy, processing speed/latency, or resilience under adversarial attack?

A3. As outlined in the SBIR, proposers are expected to detail their own proposed metrics and scope for final evaluation.

Q4. For attack-surface modeling, does DARPA expect proposals to include dynamic binary analysis of iOS/Android SMA clients, or are static reverse-engineering and fuzzing frameworks sufficient for Phase II?

A4. The program seeks novel approaches to key technical challenges, including but not limited to:

- Characterizing and modeling the attack surface of SMAs.
- Developing a framework that identifies and recommends security boundaries, protections, and mitigations for SMAs.
- Developing tools and techniques for evaluating the security features of SMAs.

Phase I feasibility will be demonstrated through evidence of: a completed feasibility study or a basic prototype system; definition and characterization of properties desirable for both Department of Defense (DoD) and civilian use; and comparisons with alternative state-of-the-art methodologies (competing approaches).

Q5. Are there quantitative benchmarks for exploit detection coverage (e.g., % of API/system call attack paths exercised) that frameworks must meet to demonstrate measurable resilience?

A5. See previous (#4) answer.

Q6. For prototype evaluation, does DARPA require integration with real-world encrypted messaging platforms (Signal, WhatsApp) in red-team trials, or is simulated attack emulation acceptable?

A6. DP2 proposals should:

- describe a proposal to achieve the aforementioned goals;
- present a technical plan and approach, with notable risks/mitigations; and
- detail proposed metrics and scope for final evaluation.

Phase II will culminate in a demonstration that shows compelling use cases consistent with commercial opportunities and/or insertion into a DARPA program which seeks to establish automated vulnerability discovery capabilities for cybersecurity applications.

Q7. Would looking at types of cyber risks beyond vulnerabilities, such as backdoor access behaviors, where data may be exfiltrated from the system, or types of interactions with the OS be in scope and of interest?

A7. The program seeks novel approaches to key technical challenges, including but not limited to:

- Characterizing and modeling the attack surface of SMAs.
- Developing a framework that identifies and recommends security boundaries, protections, and mitigations for SMAs.
- Developing tools and techniques for evaluating the security features of SMAs.

The goal of this topic is to design and develop prototype models, frameworks, and methods of evaluation to defend SMAs from real-world attacks.

DP2 proposals should:

- describe a proposal to achieve the aforementioned goals;
- present a technical plan and approach, with notable risks/mitigations; and
- detail proposed metrics and scope for final evaluation.

Phase II will culminate in a demonstration that shows compelling use cases consistent with commercial opportunities and/or insertion into a DARPA program which seeks to establish automated vulnerability discovery capabilities for cybersecurity applications.

Q8. Would looking for standard vulnerabilities (memory corruption, command injection, etc.) also need to be a focus for a strong proposal?

A8. See above (#7) answer.

Q9. Are there any particular types of cyber risks that are of the most interest?

A9. See above (#7) answer.

Q10. Are the protections and security assessments sought in this topic specifically intended for mobile devices running iOS or Android operating systems?

A10. This program does not have specific requirements for what mobile devices operating systems a SMAs should be evaluated on.

Q11. Alternatively, would a response detailing security controls or mitigations implemented at the primary server level (or within the broader system architecture) be considered acceptable for this solicitation?

A11.The program seeks novel approaches to key technical challenges, including but not limited to:

a. Characterizing and modeling the attack surface of SMAs.
b. Developing a framework that identifies and recommends security boundaries, protections, and mitigations for SMAs.
c. Developing tools and techniques for evaluating the security features of SMAs.

Q12. Can you give any specific examples for messaging apps the DoW is interested in testing?

A12. It is up to the proposer to propose which SMAs they will design and develop prototype models, frameworks, and methods of evaluation to defend SMAs from real-world attacks.

Q13. Does the DoW envision HR0011SB20254-12 being part of the ATO process?

A13. This Defense Advanced Research Projects Agency (DARPA) topic is seeking novel approaches to defend SMAs by modeling their security risks and recommending defensive measures to protect these critical platforms.

Q14. Is substantial modification to SMAs, including by adding defensive software layers, within scope of ASEMA?

A14. No.

Q15. Regarding the objective for "insertion into a DARPA program which seeks to establish automated vulnerability discovery capabilities" - are there any specific programs or technologies targeted for future integration?

A15. The solicitation does not specify a particular program. You can review many DARPA programs on the DARPA website.

Q16. Would performance on current DARPA programs with similar goals disqualify a performer from participation in ASEMA?

A16. No

Q17. Could you clarify whether the Government envisions the assessment focusing primarily on end-point/device security or the broader ecosystem (e.g., metadata leakage, traffic analysis, side-channel considerations)? How much latitude do performers have to scope their approach?

A17. The program seeks novel approaches to key technical challenges, including but not limited to:

- Characterizing and modeling the attack surface of SMAs.
- Developing a framework that identifies and recommends security boundaries, protections, and mitigations for SMAs.
- Developing tools and techniques for evaluating the security features of SMAs.

Q18. What specific transition paths or stakeholders does DARPA have in mind for ASEMA outputs? For example, are there target programs of record or interagency partners that should be considered in a transition plan?

A18. Phase II will culminate in a demonstration that shows compelling use cases consistent with commercial opportunities and/or insertion into a DARPA program which seeks to establish automated vulnerability discovery capabilities for cybersecurity applications.

Phase III work will be oriented towards transition and commercialization of this topic. The proposer is required to obtain funding from either the private sector, a non-SBIR Government source, or both, to develop the prototype software into a viable product or non-R&D service for sale in military or private sector markets. 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.

Q19. Are there particular ongoing programs or performer teams that DARPA anticipates ASEMA awardees coordinating with (e.g., related information assurance, secure comms, or AI-enabled analysis programs)?

A19. Phase II will culminate in a demonstration that shows compelling use cases consistent with commercial opportunities and/or insertion into a DARPA program which seeks to establish automated vulnerability discovery capabilities for cybersecurity applications.

Q20. Does DARPA plan to provide access to government-furnished evaluation environments or data sets for validating proposed assessment tools, or should proposers budget for building their own test infrastructure?

A20. Proposals should not rely on external resources to be successful.

Q21. Given that encrypted messaging often involves human participants, are there expected human-subject research components? If so, what are the expectations for Institutional Review Board (IRB) approvals and timelines?

Q21. No human or animal testing is expected for this research

Q22. Will any of the data sets provided or produced under ASEMA be subject to ITAR, CUI, or other restrictions? How should proposers plan for compliance and data-handling requirements?

A22. The topic is not ITAR restricted, and no CUI guide is required.

Q23. Given the maturity requirement for Direct-to-Phase II, are there expectations for higher technical readiness at project start, and does DARPA expect cost structures to differ from a standard Phase II (e.g., less time for feasibility, more emphasis on prototyping and evaluation)?

A23. This is a Direct to Phase II (DP2) solicitation. Therefore, Phase I proposals will not be accepted or reviewed. Phase I feasibility will be demonstrated through evidence of: a completed feasibility study or a basic prototype system; definition and characterization of properties desirable for both Department of Defense (DoD) and civilian use; and comparisons with alternative state-of-the-art methodologies (competing approaches). This includes determining, insofar as possible, the scientific and technical merit and feasibility of ideas appearing to have application to the core objective of creating a framework to assess the security of SMAs. Proposers interested in submitting a DP2 proposal must provide documentation to substantiate that the scientific and technical merit and feasibility described above have been met and describe the potential military or commercial applications. DP2 documentation should include:

- technical reports describing results and conclusions of existing work, particularly regarding the commercial opportunity or DoD insertion opportunity, and risks/mitigations, assessments;
- presentation materials and/or white papers;
- technical papers;
- test and measurement data;
- prototype designs/models;
- performance projections, goals, or results in different use cases

This collection of material will verify mastery of the required content for DP2 consideration. DP2 proposers must also demonstrate knowledge, skills, and ability in computer science, vulnerability research, and software engineering. For detailed information on DP2 requirements and eligibility, please refer to the DoD BAA and the DARPA Instructions for this topic.

DP2 proposals should:

- describe a proposal to achieve the aforementioned goals;
- present a technical plan and approach, with notable risks/mitigations; and
- detail proposed metrics and scope for final evaluation.

Phase II will culminate in a demonstration that shows compelling use cases consistent with commercial opportunities and/or insertion into a DARPA program which seeks to establish automated vulnerability discovery capabilities for cybersecurity applications.

Q24.What, if any, additional approaches are envisioned beyond the current industry state-of-the-art?

A24. This Defense Advanced Research Projects Agency (DARPA) topic is seeking novel approaches to defend SMAs by modeling their security risks and recommending defensive measures to protect these critical platforms.

The program seeks novel approaches to key technical challenges, including but not limited to:

- Characterizing and modeling the attack surface of SMAs.
- Developing a framework that identifies and recommends security boundaries, protections, and mitigations for SMAs.
- Developing tools and techniques for evaluating the security features of SMAs.

Q25. Is customization or extension of existing state-of-the-art capabilities appropriate for this program?

A25. Refer to question 24 response.

Q26. Have there been prior SBIRs that the team has worked on for this topic?

A26. No

1.

Q27. The solicitation focuses on frameworks to assess and defend existing SMAs. Would a proposal that demonstrates a novel SMA architecture that structurally eliminates specific attack surfaces rather than mitigating them be within scope?

A27. This solicitation is focused on analyzing the security of existing SMAs.

Q28. For DP2 feasibility documentation, does a live App Store deployment with provisional patents filed satisfy the prototype requirement?

A.28. Proposers interested in submitting a DP2 proposal must provide documentation to substantiate that the scientific and technical merit and feasibility described above have been met and describe the potential military or commercial applications. DP2 documentation should include:

- technical reports describing results and conclusions of existing work, particularly regarding the commercial opportunity or DoD insertion opportunity, and risks/mitigations, assessments;
- presentation materials and/or white papers;
- technical papers;
- test and measurement data;
- prototype designs/models;
- performance projections, goals, or results in different use cases

This collection of material will verify mastery of the required content for DP2 consideration. DP2 proposers must also demonstrate knowledge, skills, and ability in computer science, vulnerability research, and software engineering. For detailed information on DP2 requirements and eligibility, please refer to the DoD BAA and the DARPA Instructions for this topic.

Q29. Does the scope include novel transport-layer architectures that decouple voice biometric data from the communication medium entirely?

A29. The program seeks novel approaches to key technical challenges, including but not limited to:

- Characterizing and modeling the attack surface of SMAs.
- Developing a framework that identifies and recommends security boundaries, protections, and mitigations for SMAs.
- Developing tools and techniques for evaluating the security features of SMAs.

Q30. Should the framework prioritize iOS, Android, or cross-platform analysis? Are desktop SMA clients (Windows, macOS, Linux) within scope?

A30. The program is focused on the SMA. The intention is to analyze broadly applicable use cases of the SMA, so the platform environment assumed around the SMA should be consistent with the program's intention.

Q31. Beyond the attack vectors implied by the solicitation references (call establishment state machines, WebRTC implementation flaws), are there specific vulnerability classes or SMA features of particular interest to the program?

A31. The program seeks novel approaches to key technical challenges, including but not limited to:

- Characterizing and modeling the attack surface of SMAs.
- Developing a framework that identifies and recommends security boundaries, protections, and mitigations for SMAs.
- Developing tools and techniques for evaluating the security features of SMAs.

Q32. Must the framework support binary-only analysis of closed-source applications, or is source code access assumed for target SMAs?

A32. The proposal should not assume source code will be provided. If source code is accessible, it may reasonably be considered.

Q33. Is there a preference for static analysis, dynamic analysis, or a hybrid approach? Should the framework support runtime instrumentation on physical devices, emulators, or both?

A33. The focus is on the SMA and the security analysis, rather than the means of approaching it.

Q34. What level of automation is expected? Should the framework require security expertise to operate, or should it be usable by non-specialist evaluators?

A34. The program seeks novel approaches to key technical challenges, including but not limited to:

- Characterizing and modeling the attack surface of SMAs.
- Developing a framework that identifies and recommends security boundaries, protections, and mitigations for SMAs.
- Developing tools and techniques for evaluating the security features of SMAs.

Q35. Should the framework produce machine-readable outputs (e.g., SARIF, CWE mappings) for integration with existing vulnerability management systems, or are human-readable reports sufficient?

A35. The proposed framework is not required to produce machine-readable outputs.

Q36. For the Phase II demonstration, will the Government specify target SMAs for evaluation, or will proposers select representative applications?

A36. The demonstration is expected to be associated with the proposed research and framework.

Q37. The solicitation references transition into "a DARPA program which seeks to establish automated vulnerability discovery capabilities for cybersecurity applications." Can you identify the specific program name to help us align our transition planning?

A37. There may be multiple appropriate programs for transition.

Q38. Are there existing Government-furnished tools, datasets, or test environments that will be available to performers?

A38. The proposer should plan to obtain all elements required to successfully execute the proposed work. The government may provide additional resources during execution, but successful execution of the proposed plan should not be dependent on it.

Q39. For the Phase II Option period demonstration against "at least one real-world SMA," is there a preference for U.S.-developed applications, or are international SMAs (e.g., Telegram, WeChat) acceptable targets?

A39. The SMA should be broadly utilized.

Q40. Scope of "application layer" — the topic emphasizes code interacting with network and mobile OS layers, excluding cryptographic protocols. Does this extend to server-side components (message routing, key distribution servers), or is the focus strictly on client-side application code?

A40. Server-side components are in-scope.

Q41. Target SMAs — should proposers select specific applications to analyze, or is DARPA looking for a methodology that generalizes across platforms? Are there SMAs of particular interest to the program?

A41. DARPA is looking for generalizable methodologies. Proposers should select a SMA as an exemplar while showing their methodologies are useful across platforms.

Q42. Access model — for closed-source SMAs, should proposals plan around binary analysis and behavioral observation, or does the program anticipate source code access or vendor cooperation?

A42. Proposers should not anticipate vendor cooperation unless they have a pre-existing relationship with a vendor. The need for binary analysis and behavioral observation will be dependent on the proposed methodology and is acceptable but not directed.