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

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

As of 5 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.