

HR0011SB20254-03

**Multi-factor Continuous Authentication for Wearable Defense Equipment (MCAWDE)
Frequently Asked Questions (FAQs)**

1. Is the primary focus on authenticating the user to the wearable device, the device to the infrastructure, or both simultaneously?
A: Both are within scope. Proposals will be evaluated based on their specific scoping.
2. What is the minimum set of authentication factors required to meet DARPA's definition of "multi-factor"?
A: More than one. Proposals will be evaluated based on their specific scoping.
3. Are there specific interface requirements we should ensure to include in the proposal, for example for integration with the OPS-5G program, or would specific interfaces be defined upon a potential award?
A: No. proposals will be evaluated based on their specifics.
4. Are there specific power constraints or requirements?
A: The proposers are expected to identify the tradeoff between power constraints and requirements for their specific effort.
5. Is there a minimum battery life requirement?
A: The proposers are expected to identify the tradeoff between power constraints and requirements for their specific effort.
6. Are there form factor constraints, such as size and weight?
A: Form factor beyond small weight and power devices is not specified and dependent upon a proposer's specific effort.
7. Will the proposed solution need to comply with FIPS 140-3, or other NIST standards?
A: This is a Phase 3 consideration.
8. Are there specific wireless protocols that should be used or are prohibited?
A: No.
9. Will proposed solutions be allowed to have internet connectivity, or should it operate in a completely disconnected environment?
A: Both modes are within scope and will be evaluated based on a proposer's specific effort.
10. Are there specific sensor types that DARPA is most interested in, or is there a minimum number of different sensors expected?
A: No. The topic is interested in multi-factor.