SBIR: Multi-factor Continuous Authenticatio Wearable Defense Equipment (MCAWDE)

Objective Description Phase I Phase II Phase III TPOC-1

OUSD (R&E) critical technology areas: Advanced Computing and Software

Objective: The goal of Multi-factor Continuous Authentication for Wearable Defense Equipment (MCAWDE) topic is to develop and demonstrate novel, continuous, multi-factor authentication solutions for small weight and power devices.

Description: Internet-of-Things (IoT) devices have seen unprecedented growth [1] and yet remain one of the weakest links when it comes to cybersecurity [2]. User and device authentication for battery-operated IoT devices (e.g., smartphones and wearables) is challenging due to limitations on the available energy, user interface, and processing power [3].

Over the last few years, multiple authentication techniques have been developed to address these challenges, for example, location-based authentication techniques [4] and gait-based authentication techniques [5]. However, existing techniques face challenges in terms of performance overhead, power consumption, and overall efficiency of cryptographic operations [6].

To address these challenges, DARPA seeks novel, continuous [7], multi-factor authentication [8] solutions for small weight and power devices.

Phase I

The MCAWDE SBIR topic is soliciting Direct to Phase 2 (DP2) proposals only, which must include supporting documentation of Phase I feasibility.

Phase I feasibility must be demonstrated through evidence of: a completed proof of concept/principal or basic prototype; definition and characterization of properties/capabilities desirable for DoD/government and civilian/commercial use; and capability/performance

comparisons with existing state-of-the-art technologies/methodologies (competing approaches).

Entities interested in submitting a DP2 proposal must provide documentation to substantiate that the scientific/technical merit and feasibility described above has been achieved and describe the potential commercial applications. DP2 Phase I feasibility documentation should include, at a minimum:

- Technical reports describing results and conclusions of existing work, particularly regarding the commercial opportunity or DoD insertion opportunity, risks/mitigations, and technology assessments
- Presentation materials and/or white papers/technical papers
- Test and measurement data
- Prototype designs/models
- Performance projections, goals, or results in various use cases; and,
- Documentation of related topics such as how the proposed MCAWDE solution can enable multi-factor continuous authentication for wearable defense equipment

The collection of Phase I feasibility material will verify mastery of the required content for DP2 consideration. DP2 proposers must also demonstrate knowledge, skills, and abilities in the technical areas of software engineering, cyber security, privacy, analytics, and machine learning.

For detailed information on DP2 requirements and eligibility, please refer to the DoD Broad Agency Announcement and the DARPA Instructions for this topic.

Phase II

The goal of MCAWDE is to develop and demonstrate novel, continuous, multi-factor authentication solutions for small weight and power devices. MCAWDE continuous, multi-factor authentication techniques should employ lightweight device sensors to enable robust and efficient user and device authentication.

Notional proposed techniques could incorporate gait signals (captured from inertial sensors such as accelerometers and gyroscopes), heart rate sensors, and stress levels based on galvanic skin response [9, 10] to name a few. Ideally, the chosen device sensors should be relevant to or easily extensible to current devices that a warfighter might use, e.g., see [11].

Proposals are encouraged to employ multiple sensing modalities to achieve robust authentication.

Because there is a clear trade-off between the frequency of sensor readings, and power and processing overhead, any proposed solutions should require little to no user interaction for authentication. Moreover, any proposed solutions should operate in real-time and allow for privacy considerations. DP2 proposals should:

- Describe a proposed framework design/architecture to achieve the above stated goals
- Present a plan for maturation of the framework to a demonstrable prototype; and,
- Detail a test plan, complete with proposed quantitative metrics for the prototype performance

Phase II will culminate in a prototype demonstration using one or more compelling use cases consistent with commercial opportunities and/or insertion into a DARPA program, for example, the Open Programmable Secure 5G (OPS-5G) program [12], which aims, in part, to develop

techniques and security architectures enabling security at scale across devices with widely disparate size, weight, and power.

The Phase II Option period will further mature the technology for insertion into a DoD Acquisition Program, another Federal agency, or commercialization into the private sector.

The below schedule of milestones and deliverables is provided to establish expectations and desired results/end products for the Phase II and Phase II Option period efforts.

Schedule/Milestones/Deliverables: Proposers will execute the research and development (R&D) plan as described in their proposals, including the below: proposers that anticipate involving Human Subjects Research (HSR) must comply with the approval procedures .

Proposers planning to use HSR are highly encouraged to clearly segregate research tasks from human testing tasks to allow for partial funding while internal and DoD approvals are obtained.

- **Every 3 months:** Quarterly technical progress reports detailing: technical progress to date, tasks accomplished, risks/mitigations, a technical plan for the remainder of Phase II (while this would normally report progress against the plan detailed in the proposal, it is understood that scientific discoveries, competition, and regulatory changes may all have impacts on the planned work and DARPA must be made aware of any revisions that result), planned activities, trip summaries, any potential issues or problem areas that require the attention of the DARPA PM, and updates on (if applicable) Institutional Review Board and Human Research Protection Office approvals or subject enrollment when approvals are obtained.
- **Every 6 months:** Technical progress briefings to the DARPA PM (these briefings may take place as part of the OPS-5G program Principal Investigator meetings).
- **Month 24:** Final architecture with documented details; a demonstration of the ability for continuous, multi-factor authentication of wearable defense equipment; documented application programming interfaces; and any other necessary documentation (e.g., commercialization plan).
- **Month 29** (Phase II Option period): Interim report of matured prototype performance against existing state-of-the-art technologies, documenting key technical gaps towards productization.
- **Month 34** (Phase II Option period): Final Phase II Option period technical report including prototype performance against existing state-of-the-art technologies, including quantitative metrics for assessment.

Phase III dual-use applications

MCAWDE has potential applications across the DoD/government and commercially. For DoD/government, successful MCAWDE approaches are well-suited for integration into warfighter wearable devices, such as smartwatches, and tactical defense equipment. MCAWDE has the same applicability for the commercial sector.

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

MCAWDE solutions will support national efforts to help secure government, commercial, and personal IoT devices. Results of MCAWDE are intended to improve understanding of the risks

associated with the large threat surface created by IoT devices, across government and industry.

References

[1] Coughlin, Tom.IoT trends to keep an eye on in 2023 and beyond. TechTarget, IoT Agenda, 19 Jan. 2023.

[2] Dingee, Don. IoT, Not People, Now the Weakest Link in Security. DevOps.com, 23 Jan. 2019.

[3] W. M. S. Stout and V. E. Urias, "Challenges to securing the Internet of Things," 2016 IEEE International Carnahan Conference on Security Technology (ICCST), Orlando, FL, USA, 2016, pp. 1-8, doi: 10.1109/CCST.2016.7815675.

[4] Cho, G., Kwag, S., Huh, J.H., Kim, B., Lee, C., & Kim, H. (2021). Towards Usable and Secure Location-based Smartphone Authentication. SOUPS @ USENIX Security Symposium.

[5] Q. Zou, Y. Wang, Q. Wang, Y. Zhao and Q. Li, "Deep Learning-Based Gait Recognition Using Smartphones in the Wild," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3197-3212, 2020, doi: 10.1109/TIFS.2020.2985628.

[6] El-hajj M, Fadlallah A, Chamoun M, Serhrouchni A. A Survey of Internet of Things (IoT) Authentication Schemes. Sensors. 2019; 19(5):1141. https://doi.org/10.3390/s19051141.

[7] Rethinking IAM: What Continuous Authentication Is and How It Works. Ekran, 07 Dec. 2022.

[8] What is Multi-Factor Authentication (MFA) and How Does it Work? OneLogin.

[9] Yu, Wang-Yang & Wang, Shuihua & Zhang, Yudong. (2022). A survey on gait recognition in IoT applications. EAI Endorsed Transactions on Internet of Things. 7. 10.4108/eetiot.v7i28.446.

[10] Yekta Said Can, Bert Arnrich, and Cem Ersoy. 2019. Stress detection in daily life scenarios using smart phones and wearable sensors: A survey. J. of Biomedical Informatics 92, C (Apr 2019). https://doi.org/10.1016/j.jbi.2019.103139.

[11] Military wearable computing hits the mainstream. Endeavor Business Media, LLC, Military and Aerospace Electronics, 01 May 2018.

[12] Open, Programmable, Secure 5G (OPS-5G). DARPA.

Keywords

Internet of Things, Multi-Factor Authentication, Wearables, Cyber Security, Continuous Authentication, Privacy

TPOC-1:

DARPA BAA Help Desk

Email:

SBIR_BAA@darpa.mil

Opportunity

HR0011SB20254-03

Closed: Jan. 8, 2025

DoD SBIR 2025.4 | Release 2

Solicitation

Resources

- FAQs
- Topics

Contact

Embark on a journey of innovation and impact! Tell us about your interest in DARPA.
Please note: Fields marked with an asterisk are required.

Request a DARPA speaker

Full name*
Enter your full name

Email*
info@example.com

Phone number*
Enter phone number

Company / Organization*
Enter your company or organization

Your Title / Role*
Enter your title or role

Topic*
Select a Topic

Office (Optional)
Select an Office

Program Manager (Optional)
Select a Program Manager

Message*

Send Message →

Work with DARPA

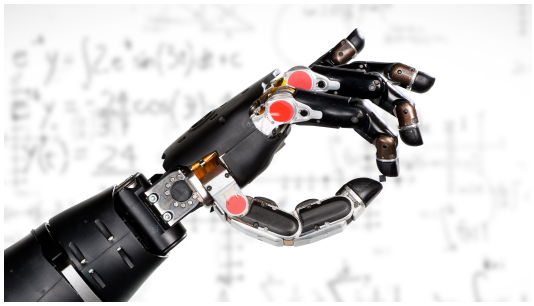
Be part of a cutting-edge research and development agency that's pushing the boundaries of what's possible, in an energetic environment with excellent benefits.

Find your future with DARPA Careers →

Our program managers are visionary leaders whose experience spans industry, government, and academia. They conceive, plan, and oversee the high-risk R&D efforts for which we are best known.

See all people at DARPA →

Research Opportunities → **View Programs** →



Redefining Possible

DARPA has pushed, and will continue to push, the boundaries of technological possibility.

See the dreams we turned to reality →

New to DARPA

Academia

Defense & Government

Investors & Entrepreneurs

Industry

Small Business

DARPAConnect

How to Respond

Programs

All Programs

Challenges

Research Spotlights

Ideas Under Incubation

Technical Offices

Biological Technologies

Defense Sciences

Information Innovation

Microsystems Technology

Strategic Technology

Tactical Technology

Support Offices

Podcast (Voices from DARPA)

Communications & Public Affairs

Features

Images Library

Case Studies

Media FAQs

Events

All Events

Rewinds

Think beyond the impossible

Explore the PM Role

Military Professionals

Contractor Information

Fellowships

Life after DARPA

About

Our Mission

Our History

Innovation Timeline

The Heilmeier Catechism

Our People

Leadership

Program Managers

Budgets and Testimony

Visitor Information

Policies | Privacy Policy | Usage Policy | Accessibility/Section 508 | No Fear Act | Webmaster | Sitemap | Visitor Information | Request a DARPA speaker | Contact

DoW Hotline | Freedom of Information Act | Information Quality | Open Government | Privacy and Civil Liberties | USA.gov