

# DARPA Calls on Industry to Assist With Improving, Strengthening DOD Cybersecurity

June 18, 2025 | By C. Todd Lopez, DOD News

The Defense Advanced Research Projects Agency announced a Resilient Software Systems Accelerator program to kick-start the widespread adoption of math-based software development practices to make military systems inherently more secure against cyberthreats.



During the Resilient Software Systems Colloquium held in Arlington, Virginia, yesterday, leaders from the Defense Department, DARPA and industry spoke about aging IT infrastructure, security standards and software tools and techniques known as "formal methods," that have been proven to significantly improve the resiliency, security and functionality of military systems used within the defense community.

Director of DARPA's Information Innovation Office Kathleen Fisher described formal methods as "mathematically based approaches" that allow the user to prove properties about software to obtain guarantees, adding that DARPA has been involved in developing tools related to formal methods for over a

decade.

Formal methods refer to techniques used to develop high-assurance, verified software, where mathematical proofs are employed to demonstrate that software on a system will behave as intended. The application of formal methods contributes to the stability and resistance of a software system to hacking.

Fisher said DARPA is eager for industry partners to get involved, which is why the agency is launching the Resilient Software Systems Accelerator. The program will provide seed funding to formal methods tool developers who partner with defense companies to apply formal methods tools and measure their level of effort to implement them.

"We are here to call you to action, to seize this opportunity and to ... motivate you to listen and to think about where you have systems at home that might benefit from formal methods," Fisher said. "DARPA is announcing today that we are going to ... offer funding to do a red team assessment of a system. You guys do this cyber retrofit and then do another red team to assess the difference, [and then] document what you did in the retrofit in a best practices standard format."

As part of advancing formal methods within DOD, DARPA is also partnering with each of the military services on a capstone demonstration of formal methods application.

Each capstone demonstration includes a red team assessment of its current state of cyber vulnerabilities followed by a formal methods retrofit, Fisher explained. Once the retrofit is completed, a follow-on red team assessment will be conducted to test system reliability.

The Air Force is starting the capstone demonstration by retrofitting software on the MQ-9 Reaper aircraft. Fisher said other services are not far behind and will soon participate in their capstone demonstrations.

During a recorded address shown at the event, Undersecretary of Defense for Research and Engineering Emil Michael said the Defense Department must now explore new ways to enhance cybersecurity.

"Our adversaries are relentless," Michael said. "So, we need systems that are resilient for today's threats and ready and adaptable for tomorrow's conflicts. That's why we are taking decisive action alongside our partners in acquisition and sustainment and DARPA."

Over the past decade, he said, DARPA and partners have worked to transform formal methods into more accessible and practical solutions than ever before.

"These advancements enable us to scale secure software systems across all DOD from legacy platforms to cutting-edge [artificial intelligence] and hypersonic technologies — defending our digital landscape," Michael said. "Yet, we have not fully harnessed this potential across the defense industrial base and DOD, leaving critical vulnerabilities unaddressed."

The colloquium brought together more than 300 leaders from DOD, industry and academia, and Michael said it fostered the collaboration needed to address the critical software challenges facing the Defense Department.

"Our goal today [is] ... to inspire widespread adoption of high-assurance formal methods, whether developed by DARPA or not," he said. "Through use cases, lessons learned and best practices, we've shown how this strengthens cyber resiliency, reduces costs and simplifies processes like securing authority to operate."

## Subscribe to Defense.gov Products

Choose which Defense.gov products  
you want delivered to your inbox.

[Subscribe](#)

Hosted by Defense Media Activity - WEB.mil