Broad Agency Announcement

Continuous-correctness On Opaque Processors (COOP) Program

MICROSYSTEMS TECHNOLOGY OFFICE

HR001124S0016

March 13, 2024

Overview Information:

- **Federal Agency Name:** Defense Advanced Research Projects Agency (DARPA), Microsystems Technology Office (MTO)

- **Funding Opportunity Title:** Continuous-correctness On Opaque Processors (COOP) Program

- **Announcement Type:** Initial Announcement

- **Funding Opportunity Number:** HR001124S0016

- **NAICS Code**: 541715

- **Assistance Listing Number:** Not applicable

- **Important Dates (All times listed herein are Eastern Time):**

  - Posting Date: **March 13, 2024**
  - Proposers Day: **March 18, 2024, 08:00 AM** Eastern Time
  - Abstract Due Date and Time: **March 28, 2024, 04:00 PM** Eastern Time
  - Question Submittal Closed: **May 03, 2024, 04:00 PM** Eastern Time
  - Proposal Due Date and Time: **May 13, 2024, 04:00 PM** Eastern Time

- **Anticipated individual awards** – Multiple awards are anticipated.

- **Types of instruments that may be awarded**:

  - Procurement contracts or Other Transactions.

- **Agency contact**

  - Technical Point of Contact: Dr. Lok Yan, Program Manager
    BAA Email: HR001124S0016@darpa.mil
    BAA Mailing Address:
    DARPA/MTO
    ATTN: HR001124S0016
    675 North Randolph Street, Arlington, VA 22203-2114

SECTION I: FUNDING OPPORTUNITY DESCRIPTION

The Defense Advanced Research Projects Agency (DARPA) Microsystems Technology Office (MTO) is soliciting innovative proposals for the Continuous-correctness On Opaque Processors (COOP) program. The COOP program seeks to develop hardware and software tools to guarantee that software is running correctly by combining formal methods and side-channels. Proposed research should investigate innovative approaches that enable revolutionary advances in science, devices, and systems. Specifically excluded is research that primarily results in evolutionary improvements to the existing state of practice.

1.1   BACKGROUND

The COOP program seeks to develop tools and techniques to continuously guarantee that software is running correctly if and only if the device physics is correct. COOP combines formal methods and side-channels to unify computer science and physics. The COOP solutions will continually guarantee software correctness on any digital processor with low overhead and falls within the category of computational integrity research. Analog and mixed-signal hardware are of interest, but only after program goals for digital hardware have been achieved.

The COOP program uses the following definitions:

- *Availability*: The ability to guarantee that data, information, processing, etc., can be accessed by authorized entities when needed.

- *Confidentiality*: The ability to guarantee that data, information, processing, etc., are not disclosed to unauthorized entities.

- *Continuous-correctness*: Informally, errors are identified and corrected within program metrics. Correctness is guaranteed over time.

- *Control boundary*: The physical and logical boundaries between what the COOP solution has full control over and what the solution has shared or no control over. Examples include, but are not limited to, power delivery and communications boundaries.

- *Correct*: Informally, a computation is correct if the output is as expected (both in time and value). Strong proposals will formalize this definition.

- *Digital-side-channel*: Manifestations of software running on hardware that are not physical. Examples include, but are not limited to, cache-based storage and timing channels. (See side-channel definition.)

- *Error*: A specific condition that leads to the computational output being incorrect (i.e., the value is incorrect, the output was not timely, or both).

- *Formal methods*: Tools and techniques that provide rigorous mathematical proofs of specified properties.

- *Informal (methods)*: Tools and techniques that are logical and rigorous but do not require mathematical proof—e.g., assumptions and qualitative arguments in English.

- *Integrity*: The ability to guarantee that data, information, processing, etc., are not altered by unauthorized entities. Correctness is a type of integrity guarantee.

- *Mission critical software (MCS)*: Any software that requires continuous-correctness guarantees—e.g., control software that directly impacts the core objectives of a mission.

- *Multi-modal-side-channel*: A combination of one or more distinct side-channels plus zero or more digital-side-channels. (See side-channel definition.)

- *Oracle*: An abstract entity used in formal methods to represent the axiomatic source of correct answers. Formal specifications and golden models are examples of oracles. Proposals must clearly describe the oracle used, why the oracle is realistic, and mitigations for if and when the oracle is proven wrong in the future.

- *Opaque*: Hardware or software is opaque if some, but not all, information about its behavior is documented and known. Examples include proprietary designs, underspecified behaviors, and erroneous documentation. While not all behaviors are known, opaque hardware and software behaviors are deterministic.

- *Processor*: Digital hardware that runs software. Examples include, but are not limited to, microcontrollers, microprocessors, and field programmable gate arrays (FPGAs).

- *Proof*: An independently verifiable argument using mathematics.

- *Reference Monitor*: A trusted entity that enforces control boundaries by completely mediating accesses. The COOP solution is a reference monitor.

- *Side-channel*: Physical manifestations of software running on hardware. Example types of side-channels include electromagnetic, power, timing, etc.

Side-channels offer a potential link between software and physics. Recent research on side-channel-based disassembly[1] demonstrated that software execution has detectable and differentiable physical manifestations. This is consistent with work on processor designs where side-channel characteristics of individual instructions could be predicted using simulations[2]. The simulators were created using models built on top of decades of research in device physics. Together, these suggest that the relationship between software execution and physics is causal and predictable, even with opaque layers in between.

Reliability physics is grounded in mathematics and can serve as the rigorous, stable, and tautological basis for formal analysis. However, side-channels can only detect errors; they cannot correct the errors. Current safety critical system design principles such as triple modular redundancy with majority voting or n-variant redundancy could continuously detect, isolate, and correct errors, but the performance penalties are prohibitive for mass deployments. New techniques that can achieve revolutionary improvements in continuous-correctness guarantees and performance are needed. Recent advances in verifiable computation and interactive proofs are promising, although higher performance is still needed.

---

[1] J. Park, et al. "Leveraging Side-Channel Information for Disassembly and Security." In ACM Journal on Emerging Technologies in Computing Systems, Volume 16, Issue 1, Article No. 6. 2019.

[2] N. Sehatbakhsh, et al. "EMSim: A Microarchitecture-Level Simulation Tool for Modeling Electromagnetic Side-Channel Signals." In Proceedings of IEEE Symposium on High-Performance Computer Architecture, 2020.

Today, formal methods can provide the strongest software correctness guarantees, but simplifying assumptions must be made to make the proofs tractable[3]. Currently, it is common to assume that lower layers in the hardware/software hierarchy are correct. Formal proofs for MCS might assume that the operating system is correct, proofs for operating systems might assume that the processor instruction set architecture is correct, proofs for the instruction set architecture might assume that the micro-architecture is correct, and so on until the proof chain reaches the physical realities of device physics. The COOP program seeks to demonstrate a formal link between MCS and physics without having to compose proofs or assume correctness across all layers.

1.2 PROGRAM DESCRIPTION

The COOP program spans two phases with program metrics outlined in Table 1.

Table 1. COOP program metrics

Metric	Phase I (18 months)	Phase II (18 months)
Multi-threaded cores support[a]	In simulation	In hardware
Correction latency	< 100 ms	< 1 ms
Performance overhead[b]	< 5x	< 2x
Error detection accuracy	99.9999999%[c]	
False positive	< 0.01%[d]	
False negative	< 0.05%[d]	

[a] Correctness techniques supports multi-threaded cores. COOP will demonstrate in simulation in Phase 1, then real multi-threaded core hardware in Phase 2.

[b] Compared to processor's native performance.

[c] Equivalent to at least 30-bits guarantee that computation is correct; the probability of not identifying an error is $\frac{1}{2^{30}}$. This will be formally verified.

[d] Assessed using IV&V designed test cases.

1.3 INFORMAL THREAT MODEL

An informal threat model of the COOP program goals and problem set is provided below. Proposals should refine the model and provide succinct informal logical arguments on the merits of their approach using the models.

1.3.1 Confidentiality, integrity, and availability in the COOP context

In COOP, a computation has integrity (i.e., it is correct) if, given an input, the output is equal to that of an oracle. The oracle can be the same computation executed in a golden processor, a formal specification, or others if defended in the proposal. Proposals must clearly and succinctly describe the chosen oracle.

Proposers do not need to guarantee data (either input or output) or computational confidentiality. Proposals should consider approaches that can support confidentiality in the

---

[3] https://sel4.systems/Info/FAQ/proof.pml

future. Proposers could propose techniques that provide confidentiality guarantees, but only after COOP goals can be achieved.

Proposers do not need to provide guarantees for data or computational availability. For example, proposers do not need to be concerned with denial-of-service (DoS) attacks caused by vulnerabilities in the opaque layers, because they exist with or without the COOP solution. Proposals should include potential mitigations against any new DoS attacks or new attack surfaces if they are introduced as part of the COOP solution.

1.3.2   COOP threat model

The COOP threat model is expected to change, as control boundaries depend on the proposed solution(s). A COOP solution (e.g., an interposer) that completely mediates all accesses (both physical and logical) between a processor and the rest of the system can assume that only the processor and non-mission critical software are untrusted, as seen in Figure 1. MCS, the COOP solution, and other computer system components/peripherals (e.g., disk) are considered trusted. However, it is important to highlight that trusted does not mean error free.

The opaque processor and non-mission critical software components are free to attempt to violate the computational integrity (correctness) of MCS as long as 1) the goal is not a DoS attack on the system, except when the DoS vulnerability was newly introduced by the proposed approach; 2) it is within the physical limitations of the components (e.g., bandwidth and power) and 3) the behavior would not render the component commercially unviable (e.g., a processor that randomly alters the output of computations is unreliable and commercially unviable).

Proposals should refine the threat model to include enhancing or relaxing the requirements to meet the needs of the proposed approach, corresponding control boundaries, and COOP goals. Proposals should clearly describe methods to identify and mitigate any new vulnerabilities or attack surfaces.
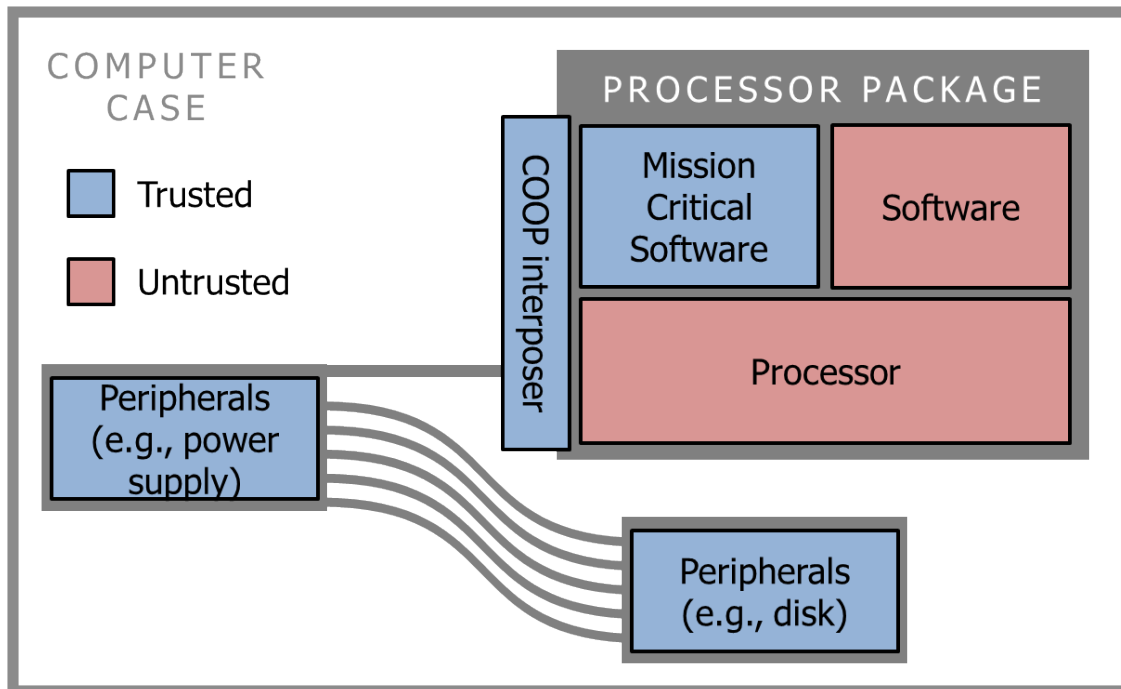
Figure 1. Trusted and untrusted components of example COOP threat model.

1.3.3 COOP boundaries

To ensure that COOP solutions can be integrated with processors that are manufactured separately, proposed COOP solutions must exist between two system boundaries. COOP solutions could reside within a processor package, but not on the same die. COOP solutions could also reside within a computer case (or equivalent), but not outside where additional resources are available, as seen in Figure 2. Proposals should consider the physical dimensions and properties of the computer system and describe how that informs the proposed solutions and formal guarantees while meeting the program goals and metrics. The informal models will change depending on the solution.
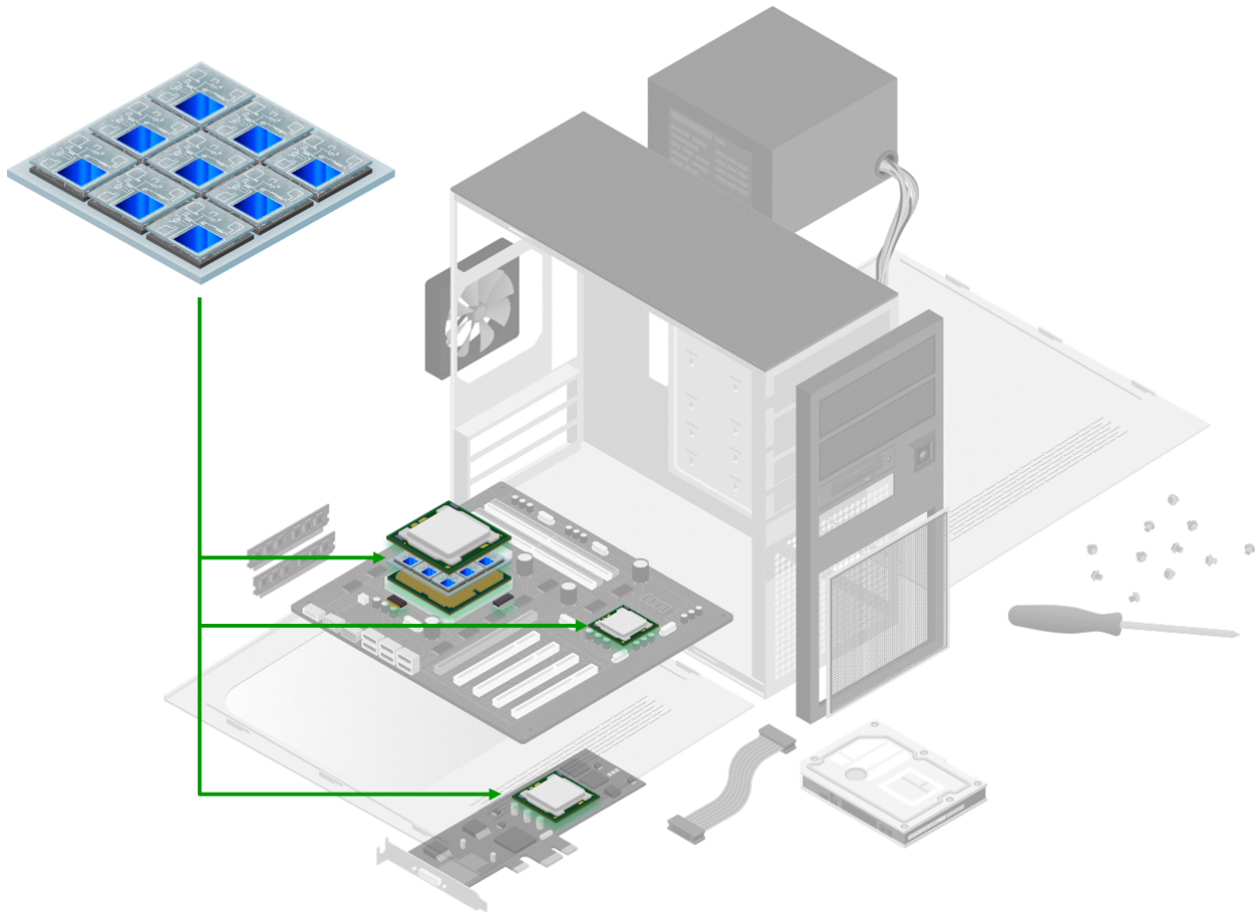
Figure 2. Potential COOP solution locations.

Potential embodiments of a COOP solution include, but are not limited to, integration within a processor's package, co-located on a board, and independently located on a daughter card. Any proposed embodiment must be able to sense multi-modal side-channels within the computer case. For simplified illustration purposes, an embodiment where COOP serves as an interposer can be found in Figure 3. This embodiment does not require an update to the control boundaries and threat model as described.

Note that Figure 3 does not represent all complexities and challenges of the COOP program. COOP seeks approaches that generalize to different types of opaque processors, such as those with multi-threaded cores or field programmable gate arrays. Each processor type might depend on support software which are also opaque, but not depicted. Proposals should describe important opaque components such as operating systems, the role they play in the overarching approach, and any additional trust assumptions if needed.
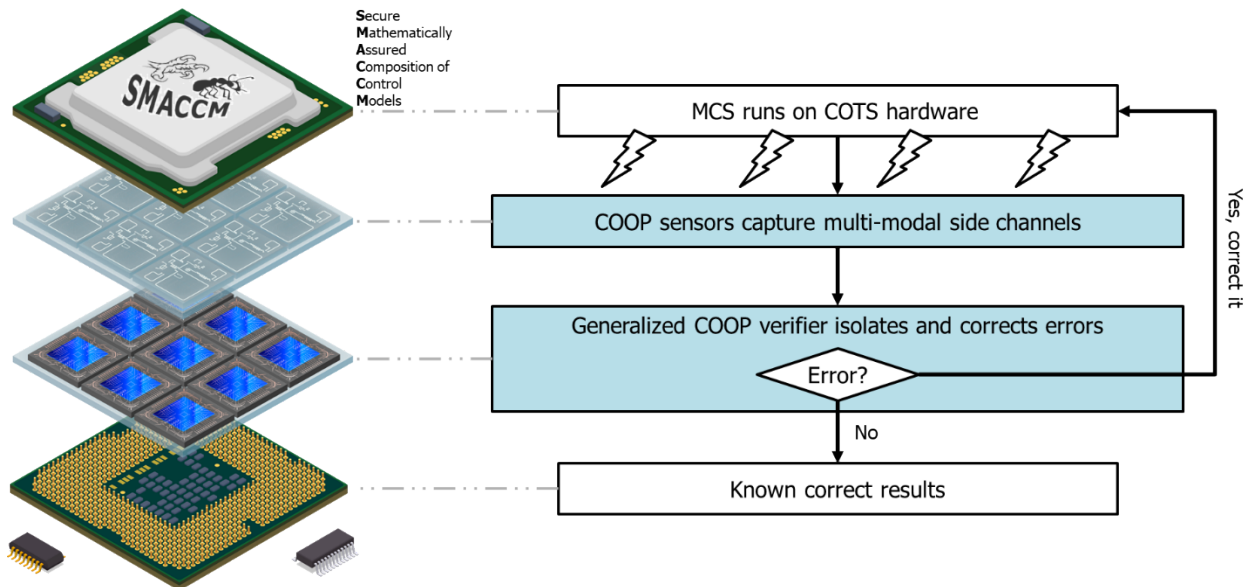
Figure 3. COOP interposer (blue layers) that continuously guarantees the correctness of MCS.

There are two program-identified technical challenges to accomplishing the COOP program goals: 1) provable physics-based software error isolation and 2) continuous provable error correction. Proposals should clearly identify and describe any additional technical challenges or steps needed to complete their technical solution.

1.3.4 Provable physics-based software error isolation

Provably isolating errors in mission critical software execution not only requires differentiating correct and incorrect outputs from the MCS, but also differentiating them from other software that are executing within the opaque processors. Modern processors are pipelined, multi-threaded, multi-core, etc., and operate with GHz clock frequencies. While there is a causal relationship between software execution and side-channels, successful error isolation should require a careful balance between sensor sensitivity, source identification, localization, data acquisition, and processing latency, amongst other variables, to meet the program metrics. The added diversity of MCS, opaque software, opaque processors, and other hardware peripherals further complicates the isolation challenge if COOP's generalizability goals are to be achieved.

The COOP program is interested in tools and techniques that can provably isolate MCS errors. Traditional approaches that use single side-channel probes and machine learning to characterize high-level MCS functions in real-time are unable to provably isolate the errors at the fine granularities needed to achieve COOP goals. On the other hand, side-channel analysis has been used to identify fine-grained information (e.g., individual bits) but at the cost of time, which does not meet COOP goals. Potential approaches include, but are not limited to, side-channel informed program synthesis, provable de-interleaving, and hardware sensor arrays.

Proposals should:

- Clearly describe the interdependencies between error isolation granularity and correction, and

- Clearly describe the provability of the error isolation.

1.3.5 Continuous provable error correction

Errors propagate through a system exponentially with time. A single bit error could propagate to the entire system in a single second if left uncorrected. In practice, error correction is limited by control boundaries, which are coupled with how fast correction can be achieved. For example, error correction code (ECC) memories can correct single bit errors for data stored in memory with zero latency, but they cannot correct errors on disk as they have no control over the disk. Similarly, speculative execution engines effectively correct mis-prediction errors by flushing the temporary state. Flushing the state limits the spread of the error to within speculation (barring vulnerabilities) with minimal overhead. Alternatively, if an error is allowed to propagate from the processor to memory (e.g., an erroneous value is written to memory), then process level checkpoint and restore could be used to correct the error but requires seconds to restore the process' state to a previous checkpoint.

The COOP program seeks solutions that can achieve provable error correction within 1 ms. Proposals should describe the correction problem with respect to control boundaries. Proposers may choose, but are not required, to solve the DoS problem in which errors are intentionally and continuously introduced into the system. However, if the solution introduces a DoS problem or new attack surfaces, it should be addressed within the proposal. Potential approaches include, but are not limited to, verifiable error-free checkpointing, speculative correction, and error-tracing for re-execution.

Proposals should:

- Clearly describe the interdependencies between error isolation granularity and correction

- Clearly describe the provability of the error correction

1.4 PROGRAM STRUCTURE

The COOP program is a 36-month, 2-phase program with an 18-month Phase I (Base) and 18-month Phase II (Option 1). The goal of Phase I is to demonstrate a COOP solution for a general-purpose processor with multi-threaded cores in simulation. The goal of Phase II is to demonstrate the generalizability of the COOP solution on general-purpose processors, graphics processing units, and/or FPGAs. Proposers should propose specific processor types for each phase and demonstration, each with increasing complexity (see Major Milestones). An independent verification and validation (IV&V) team will evaluate COOP solutions against program metrics and on corresponding processor types.

Phase I (Base) of the program will demonstrate a COOP solution on a general-purpose processor with multi-threaded cores in simulation. Proposers should specify which specific processor instance they plan to use. Proposers should anticipate having to develop formal models of the problem sets and solutions for external (e.g., IV&V and research community) scrutiny and

verification. Proposers will develop and demonstrate a solution, in simulation and in a laboratory setting, that shows that the solution is possible prior to moving onwards to Phase II. The solution shall meet the COOP metrics and the demonstrations and timelines stated in the schedule.

Phase II (Option 1) of the program will demonstrate that the COOP solution is generalizable and works in a mission-relevant environment using real hardware. Proposers should plan to fabricate and demonstrate their proposed solution on multiple different processor types that will be demonstrated and delivered to IV&V to verify the results. Proposers should describe the specific processor instances that the COOP solution will be demonstrated on. This will culminate in a mission use case demonstration that potentially uses multiple MCS on different processor types with COOP solution(s).

Two additional options should be priced for a potential Government-funded chip fabrication and packaging activity. Option 2 should include pricing for a 6-month detailed design option to bring the COOP solution to tapeout (i.e., GDSII only). Option 2 may be exercised at any time during Phase I. Option 3 should include pricing for a 7-month COOP fabrication and packaging effort. Option 3 will only be exercised after exercising Option 2. Proposers should identify a Process Design Kit (PDK) that best fits their solution and the proposed timelines for the options that meet program metrics and milestones. The Government may procure a multi-project wafer (MPW); however, no specific PDK has been identified. Options may be exercised, at the Government's sole discretion, based on technical progress measured against the metrics and milestones defined in the BAA and funding availability.

1.5 SCHEDULE/MILESTONES

The Government will specify the locations for quarterly program reviews, demonstrations, and kickoff/PI meetings after program kickoff. For budgeting purposes, proposers may assume that quarterly program reviews will alternate between Arlington, VA, and San Diego, CA, for two days at a time. The overall program schedule is depicted in Figure 4. The COOP program intends to use planned demonstrations to verify and validate the theory and practicality of proposed approaches. Proposals should include a constructive technical plan for how the technical approach ties in with the schedule and builds upon earlier development, deliverables, and demonstrations.
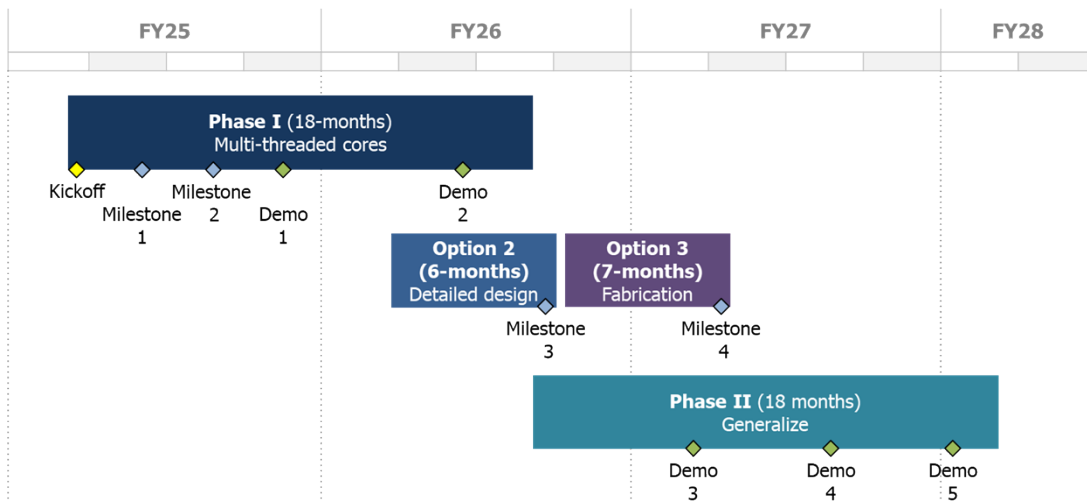
Figure 4. COOP program schedule

Major Milestones:

- Kickoff: 1 month post contract award (PCA)

- Quarterly Program Reviews: Every 3 months after program kickoff

- Milestone 1: Formal models and specifications for error isolation – 4 months PCA

- Milestone 2: Formal models and specifications for error correction– 7 months PCA

- Demo 1: Demonstrate COOP solution on a general-purpose processor – 9 months PCA

- Demo 2: Demonstrate COOP solution on general-purpose processor with multi-threaded cores – 15 months PCA

- Milestone 3: Models, specifications, and physical COOP design – 20 months PCA

- Demo 3: Demonstrate COOP solution on a second processor (e.g., a high-performance processor) – 25 months PCA

- Milestone 4: COOP solution delivery – 27 months PCA

- Demo 4: Demonstrate COOP solution on a third processor (e.g., an FPGA) – 31 months PCA

- Demo 5: Demonstrate COOP on DoD relevant mission critical software – 34 months PCA

1.6   DELIVERABLES

Proposers are responsible for providing the following deliverables:

- Slide Presentations – Final slide presentations are due no later than 48 hours before the program kickoff meeting and each review.

- Monthly Financial Reporting – Each team must submit monthly expenditure reports and any associated deliverables within fifteen (15) calendar days after the end of each calendar month.

- Monthly Technical Status Report – A monthly technical status report is due within fifteen (15) calendar days after the end of each calendar month. The report must describe technical progress made, progress towards metrics, resources expended, and any issues that require the attention of the Government team and shall not exceed six (6) pages.

- Quarterly Program Review – Each team will attend a quarterly program review that provides technical status, resources expended, and progress towards metrics.

- Phase and Final Technical Reporting – End-of-phase reports are due at the conclusion of each phase. A separate Final Technical Report is due at the end of the period of performance. The reports will concisely summarize the effort conducted and provide any lessons learned during the development of the technology.

- Software – All computer software developed or utilized during the program must be delivered as source and executable code unless otherwise prohibited, such as through rights assertions. The source versions and source code for the target computer systems, as well as any build scripts or other technical information required for the Government to compile and configure all delivered source code, must also be included. Delivered software under this effort is to be maintainable and modifiable with no reliance on any non-delivered computer programs or documentation. Software is expected to be delivered utilizing continuous delivery and integration methods. At the end of each phase, software deliverables must also include unit tests to help the Government quickly determine whether the software is running as expected.

- Software Documentation – Software documentation deliverables are due ten (10) calendar days after each software delivery. Documentation must describe the source code, build system, hardware description language specifications, system diagrams, part numbers, and any other data necessary to build, maintain, and produce copies of the software.

- Hardware – All hardware procured or developed under the program will be delivered to the Government. The delivery should include sufficient documentation to be completely operable, maintainable, and modifiable with no reliance on any non-delivered hardware or hardware documentation. The delivery should also include unit tests to help the Government quickly determine whether the hardware is running as expected.

1.7 GOVERNMENT FURNISHED EQUIPMENT/PROPERTY/INFORMATION

DARPA does not intend to provide equipment, facilities, property, or information. However, if DARPA procures a Government multi-project wafer run, the chips designed by performers will be provided as Government Furnished Property.

1.8 INTELLECTUAL PROPERTY

It is strongly desired that the data and software delivered under COOP is provided with Unlimited Rights or with Government Purpose Rights (GPR) at a minimum. Proposers are further encouraged to provide data rights that enable sharing, such as through open-source licenses, to provide a foundation for the community to continuously expand and grow the tools.

SECTION II: EVALUATION CRITERIA

Proposals will be evaluated using the following criteria listed in *descending order of importance*: Overall Scientific and Technical Merit; Potential Contribution and Relevance to the DARPA Mission; and Cost and Schedule Realism.

- **Overall Scientific and Technical Merit:**
  The proposed technical approach is innovative, feasible, achievable, and complete. Detailed technical rationale is provided delineating why the proposed approach can achieve the program goals and metrics. The proposed technical team has the expertise and experience to accomplish the proposed tasks. Task descriptions and associated technical elements provided are complete and in a logical sequence with all proposed deliverables clearly defined such that a final outcome that achieves the goal can be expected as a result of award. The proposal identifies major technical risks, and planned mitigation efforts are clearly defined and feasible. All prior research leveraged in order to obtain the maximum benefit from the available funding is relevant, clearly substantiated, and not duplicated.

- **Potential Contribution and Relevance to the DARPA Mission:**

  The potential contributions of the proposed effort bolster the national security technology base and support DARPA's mission to make pivotal early technology investments that create or prevent technological surprise. The proposed intellectual property restrictions (if any) will not significantly impact the Government's ability to transition the technology.

- **Cost and Schedule Realism:**
  The proposed costs are realistic for the technical and management approach and accurately reflect the technical goals and objectives of the solicitation. The proposed costs are consistent with the proposer's Statement of Work and reflect a sufficient understanding of the costs and level of effort needed to successfully accomplish the proposed technical approach. The costs for the prime proposer and proposed sub awardees are substantiated by the details provided in the proposal (e.g., the type and number of labor hours proposed per task, the types and quantities of materials, equipment and fabrication costs, travel and any other applicable costs and the basis for the estimates). The effort leverages all available relevant prior research in order to obtain the maximum benefit from the available funding.

Unless otherwise specified in this announcement, for additional information on how DARPA reviews and evaluates proposals through the Scientific Review Process, please visit: Proposer Instructions and General Terms and Conditions.

SECTION III: SUBMISSION INFORMATION

- This announcement allows for multiple award instrument types to be awarded to include <u>Procurement Contracts</u> and <u>Other Transactions</u>. Some award instrument types have specific cost-sharing requirements. The following websites are incorporated by reference and contain additional information regarding overall proposer instructions, general terms and conditions, and each specific award instrument type.

    o **Proposer Instructions and General Terms and Conditions**: <u>Proposer Instructions and General Terms and Conditions</u>

    o **Procurement Contracts**: <u>Proposer Instructions: Procurement Contracts</u>

    o **Other Transaction agreements**: <u>Proposer Instructions: Other Transactions</u>

- This announcement contains an abstract phase. Abstracts are strongly encouraged but not required. Abstracts are due <u>March 28, 2024, at 4:00 PM Eastern Time</u> as stated in the Overview section. Additional instructions for abstract submission are contained within **Attachment A**.

- Full proposals are due <u>May 13, 2024 at 04:00 PM Eastern Time</u> as stated in the Overview section. **Attachments B, C, D, and E** contain specific instructions and templates and constitute a full proposal submission. Please visit <u>Proposer Instructions and General Terms and Conditions</u> for specific information regarding submission methods through the Broad Agency Announcement Tool (BAAT).

- **BAA Attachments**:
    o **Attachment A** - Abstract Instructions and Template
    o **Attachment B** - Proposal Summary Slide Template
    o **Attachment C** - Volume I: Technical and Management Proposal Volume Template
    o **Attachment D** - Volume II: Cost Volume Template
    o **Attachment E** - MS Excel™ DARPA Standard Cost Proposal Spreadsheet
    o **Attachment F** - Associate Contractor Agreements
    o **Attachment G** - MTO Controlled Unclassified Information Guide signed 11/03/2023
    o **Attachment H** – Other Transaction Certification Template

SECTION IV: SPECIAL CONSIDERATIONS

- This announcement, stated attachments, and websites incorporated by reference constitute the entire solicitation. In the event of a discrepancy between the announcement, attachments, or websites, the announcement shall take precedence.

- All responsible sources capable of satisfying the Government's needs, including both U.S. and non-U.S. sources, may submit a proposal that shall be considered by DARPA. Historically Black Colleges and Universities, Small Businesses, Small Disadvantaged Businesses and Minority Institutions are encouraged to submit proposals and join others in submitting proposals; however, no portion of this announcement will be set aside for

these organizations' participation due to the impracticality of reserving discrete or severable areas of this research for exclusive competition among these entities. Non-U.S. organizations and/or individuals may participate to the extent that such participants comply with any necessary nondisclosure agreements, security regulations, export control laws, and other governing statutes applicable under the circumstances.

- As of the time of publication of this solicitation, all proposal submissions are anticipated to be unclassified.

- This program is subject to Attachment F - Associate Contractor Agreements. The success of COOP hinges upon continuous collaboration across COOP performers. Therefore, any resultant COOP award will contain a term/condition pursuant to the stipulations outlined in Attachment F.

- This program is subject to Attachment G - MTO Controlled Unclassified Information (CUI) Guide signed November 03, 2023. All individuals accessing CUI agree to protect CUI in accordance with *DoD Instruction 5200.48 CONTROLLED UNCLASSIFIED INFORMATION (CUI)* and *NIST Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*.

- Federally Funded Research and Development Corporations (FFRDCs), University Affiliated Research Centers (UARCs) and Government entities interested in participating in the COOP program or proposing to this BAA should first contact the Agency Point of Contact (POC) listed in the Overview section prior to the Abstract due date to discuss eligibility. Complete information regarding eligibility can be found at Proposer Instructions and General Terms and Conditions.

- As of the date of publication of this solicitation, the Government expects that program goals as described herein either cannot be met by proposers intending to perform fundamental research or the proposed research is anticipated to present a high likelihood of disclosing performance characteristics of military systems or manufacturing technologies that are unique and critical to defense. Therefore, the Government anticipates restrictions on the resultant research that will require the awardee to seek DARPA permission before publishing any information or results relative to the program. For additional information on fundamental research, please visit Proposer Instructions and General Terms and Conditions.

Proposers should indicate in their proposal whether they believe the scope of the research included in their proposal is fundamental or not. While proposers should clearly explain the intended results of their research, the Government shall have sole discretion to determine whether the proposed research shall be considered fundamental and to select the award instrument type. Appropriate language will be included in resultant awards for non-fundamental research to prescribe publication requirements and other restrictions, as appropriate. This language can be found at Proposer Instructions and General Terms and Conditions.

For certain research projects, it may be possible that although the research to be performed by a potential awardee is non-fundamental research, its proposed sub-

awardee's effort may be fundamental research. It is also possible that the research performed by a potential awardee is fundamental research while its proposed sub-awardee's effort may be non-fundamental research. In all cases, it is the potential awardee's responsibility to explain in its proposal which proposed efforts are fundamental research and why the proposed efforts should be considered fundamental research.

- DARPA has utilized an alternate structured approach for the determination of a reasonable fee basis for Cost-Plus-Fixed-Fee (CPFF) procurement contracts under COOP, in accordance with DFARS 215.404-4(b)(1)(C). **The fee calculation percentage range determined reasonable for procurement contract awards under COOP is 6.0% - 8.8%**. This was determined based on consideration of factors such as: performance risk; contract type risk; facilities capital employed; anticipated award size; available transition path; markets (commercial, Government, international); IP rights; chances of award; time to production; and solicitation complexity.

  Proposers seeking a CPFF procurement contract should propose a fee that falls within the above range. Because that fee range already has been determined to be reasonable relative to COOP, proposals need not include any further fee justification. Elimination of fee as a negotiation item is expected to result in reduced contracting timelines for any proposal selected for award negotiation. It should be noted that this structured approach only applies to CPFF procurement contracts and not to other transactions.

- Prospective proposers can request the proposer's day attendee list and/or the prospective proposer profile list through email at DARPA-SN-24-41@darpa.mil. All email requests must be received by 1:00PM ET on March 29, 2024, and follow the same security requirements as proposer's day attendees (e.g., government photo ID and DARPA Form 60 requirements). It is incumbent on email requesters to ensure all provided information is accurate. DARPA will not provide access to secure data transfer capabilities (e.g., DoD Safe) and DARPA reserves the right to deny requests stemming from its vetting of requesters' security documentation.

- DARPAConnect offers free resources to potential performers to help them navigate DARPA, including "Understanding DARPA Award Vehicles and Solicitations", "Making the Most of Proposers Days", and "Tips for DARPA Proposal Success". Join DARPAConnect at www.DARPAConnect.us to leverage learning and networking resources.

- DARPA has streamlined our Broad Agency Announcements and is interested in your feedback on this new format. Please send any comments to DARPAsolicitations@darpa.mil