
# Broad Agency Announcement

# Information Innovation Office

## Reclaiming Bus-based Systems During Compromise (Red-C)

HR001125S0005

January 29, 2025

This publication constitutes a Broad Agency Announcement (BAA) as contemplated in Federal Acquisition Regulation (FAR) 6.102(d)(2) and 35.016 and 2 CFR § 200.203. Any resultant award negotiations will follow all pertinent law and regulation, and any negotiations and/or awards for procurement contracts will use procedures under FAR 15.4, Contract Pricing, as specified in the BAA.

# SECTION I: OVERVIEW INFORMATION

- **Federal Agency Name** – Defense Advanced Research Projects Agency (DARPA), Information Innovation Office (I2O)
- **Funding Opportunity Title** – Reclaiming Bus-based Systems During Compromise (Red-C)
- **Announcement Type –** Initial Announcement
- **Funding Opportunity Number –** HR001125S0005
- **Assistance Listing Number:**
- **Dates/Time - All Times are Eastern Time Zone (ET)**
    - Posting Date: January 29, 2025
    - Proposers Day: January 28, 2025
    - Question Submittal Closed: March 6, 2025 at 5:00 PM ET
    - Proposal Due Date: April 10, 2025 at 5:00 PM ET
- **Anticipated individual awards** - Multiple awards are anticipated.
- **Types of instruments that may be awarded** – Procurement Contracts, Cooperative Agreements, and Other Transactions for Prototype
- **NAICS Code**: 541715
- **Agency contact**

  Point of Contact
    - The BAA Coordinator for this effort may be reached at:
      RedC@darpa.mil

      DARPA/ I2O
      ATTN: HR001125S0005
      675 North Randolph Street
      Arlington, VA 22203-2114

## SECTION II: DEFINITIONS

Table 1 provides the definitions for terms used throughout this Broad Agency Announcement (BAA).

*Table 1: Red-C program definitions*

| Term | Definition |
|---|---|
| **Sensor** | A device which detects or measures a physical property and records, indicates, or otherwise responds to it [1] |
| **Component** | A component is a sub-system on a bus with a designated purpose that may include sensors, memory, data storage, commutation, etc.<br>• GPU and SSD controllers are examples of components for the PCIe bus<br>• Engine control and power steering module are examples of CAN bus components |
| **System** | A system is comprised of components (e.g., personal computer, vehicle) |
| **Forensic Observation Data (FOD)** | Component or system information enabling detection, repair, or inoculation, for example:<br>1. Low resolution granular signal of component(s) state and/or behavior<br>2. Historical informing of past known local and global good states<br>3. Data informing the vulnerabilities used by the attacker and/or the path through the cyber kill chain the attacker used |
| **Forensic value** | Forensic data that is unique (e.g., illustrates a relevant distinct property) and immutable (e.g., the meaning of the data will not change over a known time span) |
| **Coverage of a bus** | A sufficient number of critical components which enable redundant (two or more) components' FOD generation for all processes on the bus. |
| **Zero-Trust** | Each of the components is monitoring its peers to detect, repair, and inoculate |
| **Attestation** | Evidence or proof of something, not strictly encryption |
| **Red-C Model** | Software written in python to replay/simulate Red-C datasets and bus messages under various experimental conditions (e.g., computational constraints, bus bandwidth constraints, timing, ect.) enabling algorithm development |
| **Red-C Compliant** | Firmware with the functionality of either TA1 and/or TA2, which is interoperable with all other Red-C compliant firmware |
| **Open-Source** | Publish to the internet with a license that does not restrict commercial or academic use by other parties (e.g., the MIT License) in two or more locations (i.e., Test and Evaluation Team website and another code repository e.g., GitHub) |
| **Detection** | Identification of cyber attack(s) and the affected component(s) |
| **Repair** | A global and local state change of a system and/or component(s) ensure the system is in a valid state |

| | |
|---|---|
| **Inoculate** | A code or configuration change which removes the attacker's ability to exploit the initial attack vector. (synonym: Strategic Patching) |
| **Response** | Detection, Repair, and Inoculation |
| **SOTA** | State of the Art |
| **LLMs** | Large Language Models |
| **NIC** | Network Interface Card |
| **SSD** | Solid State Drive |
| **PCIe** | Peripheral Component Interconnect Express bus |
| **CXL** | Compute Express Link bus |
| **CAN** | Controller Area Network bus |
| **API** | Application Programming Interface |
| **AMP** | DARPA's Assured Micropatching program |

[1] Source: Google Oxford Languages

# SECTION III: FUNDING OPPORTUNITY DESCRIPTION

The Defense Advanced Research Projects Agency (DARPA) is soliciting innovative proposals in the following technical areas: cyber, resilience, systems, buses, and Zero Trust[1]. Proposed research should investigate innovative approaches that enable revolutionary advances in science, devices, or systems. Specifically excluded is research that primarily results in evolutionary improvements to the existing state of practice.

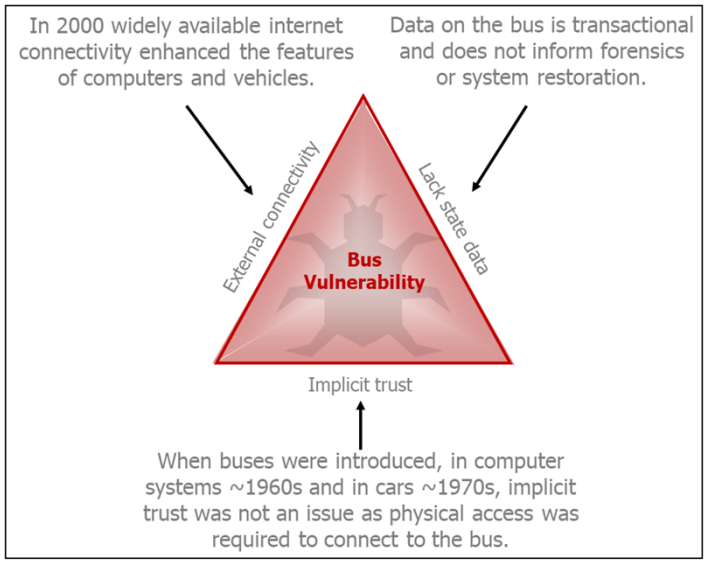
## Program Goal

Reclaiming Bus-based Systems During Compromise (Red-C) will explore algorithms to construct self-healing systems, by retrofitting firmware for individual components on a bus to function as forensic sensors that collectively monitor peers to detect, repair, and inoculate on-system during a cyber-attack.

## Program Introduction

Many Department of Defense (DoD) critical systems[2] are bus-based systems of systems with implicitly trusted modular components. Bus-based systems are currently vulnerable to cascading implicit trust attacks (e.g., any door or window gains access to the whole house), and system recovery is hindered by the lack of available forensic information (e.g., we know files have been corrupted, but not their original content). To end the lack of state data and the cascading implicit trust flaw in modern buses, a resilient approach to on-system detection and repair of cyber-attacks is needed that can be implemented on current hardware via firmware updates.

Figure 1 illustrates compound effect of design choices over time on bus security.




[1] According to the DoD Zero Trust Strategy, Zero Trust is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.

[2] Example systems include vehicles which typically have engine control modules, power steering modules, etc. and personal computers which typically have memory controllers, graphic processing units, disk controllers, etc.

*Figure 1: History of bus design led to today's cyber security landscape (Source: DARPA)*

The Reclaiming Bus-based Systems During Compromise (Red-C) program seeks to recover a system after one or more components on the bus have been compromised. Red-C is a late-stage cyber-attack recovery program, wherein even after successful compromise the system integrity can be restored and the antagonist removed in the last act. Red-C will construct a neighborhood watch for components connected via communication highways, known as buses, by turning components into forensic sensors with introspection and cooperative agreement, via Zero Trust, to enable on-system recovery from cyber-attacks, thus ensuring mission continuity.

Figure 2 illustrates an overview of the program.

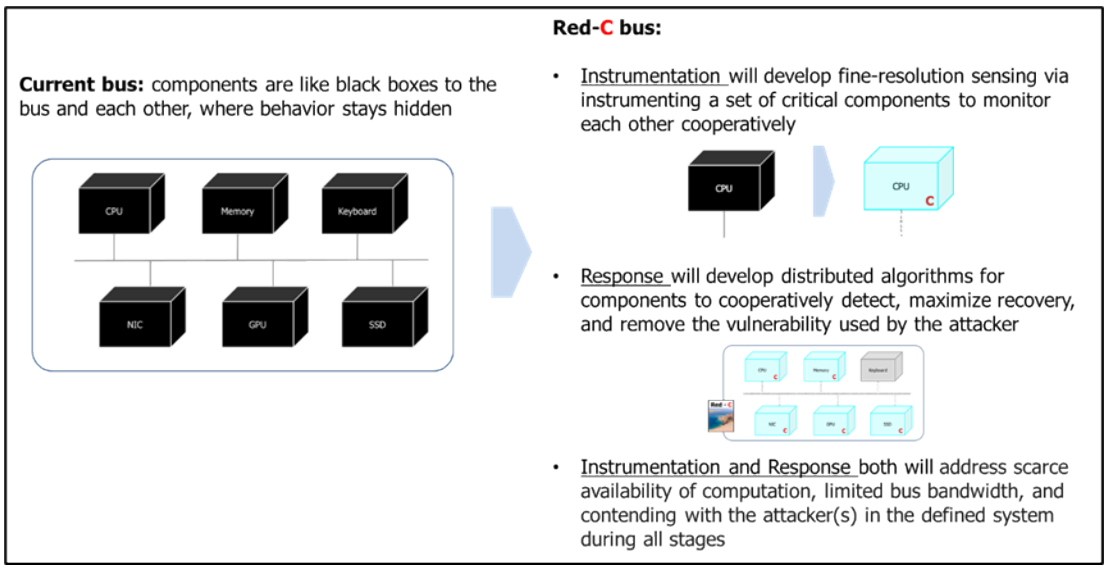



*Figure 2: Red-C program overview (Source: DARPA)*

Modern buses provide super-highways, which are crossed multiple times by all processes on a system to reach numerous specialized components and leverage their resources, such as computation and memory. These processes leave behind an ever-growing forensic footprint and provide a way for neighbors to collectively detect, repair, and remove the vulnerability used by the attacker. Red-C's approach capitalizes on this to create self-healing systems, through two technical areas:

- Technical Area 1 (TA1): Instrumentation ensures the neighbors in the neighborhood watch are observant and trustworthy. The aggregation of low-level independent signals that can be gained from the instrumentation of components provides a global perspective, which illuminates system behavior, adding a new level of resolution to bus monitoring.

- Technical Area 2 (TA2): Response must be locally generated via a distributed approach to enable timely remediation, mitigating further damage, and must inform inoculation of the system from vulnerabilities used in the cyber-attack. Response can use the valuable forensic data provided by TA1's instrumentation to inform detection, repair, and inoculation.

The collective effect is that Red-C imposes a cost to the attacker, penalizing the use of an attack, as trying or using the door ensures it is locked next time.

**Program Structure**

The Red-C program will address several main research thrusts and global technical challenges:

- Main research thrusts:
  - Develop fine-resolution sensing via instrumenting a set of critical components to monitor each other cooperatively, leading to a powerful forensic capability not available today
  - Develop distributed algorithms for components to act independently in a range of tasks from attack detection to maximal recovery
  - Demonstrate online bus reclaiming and firmware retrofitting, thus putting an end to the cascading implicit trust flaws in modern buses
- Global technical challenges:
  - Create robust distributed algorithms with scarce availability of computation and limited bus bandwidth
  - Contend with the attacker(s) in the defined system during all stages

Addressing the research thrusts and global technical challenges will require new algorithms and modified firmware that demonstrates the new algorithms. Red-C is soliciting novel approaches to automated on-system reactive cyber defense.

Red-C is a single-phase program that will produce prototype firmware systems and Red-C models, including implementations of algorithms in python and various experimental control code. Red-C is focused on creating Technology Readiness Level (TRL) 6 prototype systems, enabling the collection of datasets and a true benchmark for performance. The program will open-source datasets and Red-C models to enable community contribution and lower the barrier for authoring Red-C compliant firmware. All components shall be at the unclassified level and strong proposals will cover systems with large shares of a relative market (e.g., PCIe Windows operating system).

Red-C will only consider publicly available PCIe or CXL bus-based systems in scope. Proposals requiring any modification to hardware are out of scope; Red-C will not develop hardware. Proposers shall clearly state their access to source code or ability to repackage firmware, access to hardware, and their ability to reflash firmware. Performers shall purchase hardware instances for two systems: one for development and one for the Test and Evaluation (T&E) Team as a test platform. Proposers should clearly describe their plan to reach TRL 6 within two years.

A key objective of Red-C is to create a symbiotic community of component developers and algorithm researchers by accurately documenting the state of current algorithmic development, documenting the remaining open problems, and providing the greater Computer Science community with the tools and datasets needed to solve fundamental algorithmic challenges in Red-C models. Advances in algorithms can and should be ported back into Red-C firmware.

To facilitate Red-C's objective of creating a symbiotic community, we will focus our collective attention to the PCIe and CXL buses, write our Red-C models in python, and publish (algorithms, datasets, and models) with a Red-C appropriate open-source license on the public-facing program website, bus-watch.org. Proposers should specify a license that does not restrict commercial and academic use by other parties. Licenses like the MIT License are strongly preferred. If other licenses are proposed, proposers should provide a rationale for why the license meets Red-C program goals. Bus-watch.org is planned to be a scikit-learn-like environment that will house

performers' datasets, algorithms developed, and model implementations of their algorithms[3], including necessary supporting code[4] and will be hosted by the T&E Team.

The Red-C focus on firmware to create self-healing systems ensures its application to legacy systems and will drive algorithm development. The viability of Red-C is directly linked to having enough forensic coverage and density of forensic data to ensure system processes are observed and the signal generated does not exceed a nominal overhead on normal operation.

Red-C will enter the cybersecurity ecosystem. Therefore, consideration must be given to ensuring that Red-C does not introduce new vulnerabilities into this ecosystem.

Firmware created on proprietary hardware during Red-C will be the intellectual property of the performer and not a deliverable. Firmware created on open-source hardware shall be open-sourced. The T&E Team will verify that the open-source implementation and algorithms delivered are congruent with the firmware implemented. All proposals shall explicitly state that all work performed under Red-C will be published to the Red-C program website, bus-watch.org, including descriptions of the fundamental algorithmic challenges and how they were addressed[5].

Red-C program development was informed by a seedling known as Late-Stage Cyber-Attack Recovery (LastAct). This seedling was TRL3 and partially achieved the goals of TA1: Instrumentation and attestation. Using labeled data and a reserved testing dataset, LastAct achieved 99% detection of ransomware and 92% detection of botnet denial of service attacks while only adding 6% additional component computational overhead. The dataset from the LastAct seedling will be released with the BAA. Please see the program website at bus-watch.org. The LastAct seedling data is only provided as one datapoint for a state-of-the-art (SOTA) baseline. The metrics listed in Table 3 state that a validation set of previously unseen samples will be used for scoring Red-C.

All proposals should clearly describe the key innovations that can meet the goals of their respective technical area and present arguments and evidence for the potential to meet metrics listed in Table 2 and milestones shown in the program schedule in Figure 2.

**Technical Areas**

Red-C will develop and demonstrate technologies in the following technical areas:

- TA1: Instrumentation
- TA2: Response
- T&E (included for information purposes only)

DARPA anticipates funding multiple technical approaches and proposers for TAs 1 and 2. T&E information is included in this solicitation for information only; proposals for T&E will not be accepted. The individual TAs are elaborated below. Proposers may respond to one or both TA1 and/or TA2 but must submit separate proposals for each TA.

---

[3] Code may be provided in a Jupyter notebook

[4] For example: model functionality to replay datasets under various experimental conditions

[5] Red-C Compliance may be defined by a standard of what data is published to the bus and what parser functionality is needed. However, performers must publish to the bus-watch.org website the fundamental problem of how to dynamically integrate new data types into a Red-C ecosystem.

**TA1 - Instrumentation:**

Each component on a bus has some degree of compute, memory, storage, interconnectivity, etc. and can generate Forensic Observation Data (FOD), which informs component and system states, enabling on-system detection, repair, and inoculation. TA1 shall rewrite/modify firmware of a component to generate FOD. With respect to the existing hardware of a component, the FOD shall be transmitted on the bus and utilized locally.

All forensic data shall be both unique (illustrating a distinct property of the component with respect to the systems) and immutable (the value of the data is invariant over a known time window).

- FOD for detection should create a low-resolution granular signal of component behavior.
- FOD for repair should enable recovery to a functional, global and local, state or assist in identifying affected services and processes.
- FOD informing the automated creation of strategic patches should contain system behavior exposing information on the vulnerability(ies) used by the attacker.

Strong proposals will indicate FOD value with respect to the three types of data, ensure forensic density where superfluous information is not stored or sent on the bus, and minimize bus bandwidth and component computational overhead.

Red-C should only use attestation when the addition of attestation directly and quantifiably benefits TA2. TA1 proposals which simply use version numbers, trusted boot, trusted certificates, or encryption where the key is stored in unprotected memory are out of scope. TA1 shall provide coverage of a bus, ensuring a sufficient number of critical components are made Red-C compliant, enabling redundant FOD generation where two or more components will create FOD for all processes.

**TA2 – Response:**

The overall interrelated goals of TA2 – detection, repair, and inoculation leveraging TA1 FOD – enable self-healing bus-based systems. TA2 proposals shall address all TA2 goals; approaches to any one goal which reduce the complexity of the remaining goals are welcome.

TA2 proposals shall outline the approach to providing formal guarantees of properties claimed for distributed Zero Trust algorithms. For example, in the case of a Byzantine General's mutual agreement algorithm, proposals must first identify what the guarantee is and when it holds and prove how all relevant preconditions are met.

To focus on the core program challenges, several approaches are out of scope:

- Approaches for detection or repair which require centralized control (i.e., one component makes critical decisions and cannot be removed)
- Approaches requiring off-system communication for in mission function
- Approaches for detection that only utilize anomaly detection
- Approaches that leverage machine learning and do not prove they are robust in all use cases (e.g., vulnerable to known attacks, for example perturbation attacks)

### TA2.1 - Detection

Most bus-based systems have disparate component capabilities with respect to compute, memory, storage, etc. Accurate on-system detection via a disparate distributed zero-trust architecture, where each of the components is monitoring its peers, shall use the minimal amount of bus bandwidth and component overhead. Each Red-C enabled component should be leveraged with respect to its hardware resource to contribute to detection, repair, and inoculation. Detection should inform the bus-based system user and shall initiate automated responses. Red-C shall pursue automated responses as they present key algorithmic challenges, however limited user interactions could be used in targeted cases. Proposers should clearly identify when, how, and why solutions would incorporate user interactions.

Proposals shall clearly describe in detail the open research challenges and their novel approaches. For example, discovering previously unseen (zero-day) malware is a known open problem. TA2.1 Red-C baseline may consist of SOTA methods of detection (e.g., anomaly detection, heuristics, and hashes of known samples), however these are not considered novel approaches for malware discovery. TA2.1 should address the research challenges in aggregating untrusted fragmented forensic signals into a global system state.

### TA 2.2 – Repair

Automated on-system repair should recover the maximum functionality of a system, collect vital information that informs strategic patching, and most critically, shall not introduce additional vulnerabilities. Repair strategies should consider restoring system control and ensuring a minimum degradation to the system. TA2.1 and TA2.2 should continue to gain FOD to enable forensic investigation. TA1 FOD collected during detection may be leveraged for design of repair.

TA2.2 repair will address fundamental challenges such as:

- Determining if sufficient data is available to ensure a viable restoration
- Determining the point in time and a known valid state for system restoration
- Ensuring local component(s) repairs are globally and locally viable
- Ensuring the repairs to a predetermined determined state are not more damaging than remaining in the current state

Approaches may include combining distributed algorithms with processing chronology TA1 FOD to address these challenges.

### TA2.3 – Inoculation

TA2.3 will automate on-system strategic patch generation, which will change code and/or configurations to remove the attacker's ability to exploit the initial attack vector. Red-C systems should inoculate all components affected by a cyber-attack via automated methods. Strategic patches may degrade the system in a limited pre-determined manner[6]. In some DoD applications, allowing short term continued function at the risk of long-term system damage may be necessary and should be able to be calibrated. Proposals should detail their range of approaches to

[6] For example, for PCIe defining a minimum set of Intelligent Platform Management Interface (IPMI) APIs which can be used under specific attack detection types to remove effected attack surfaces.

inoculation; for example, predetermined configuration changes to on-system patch generation and patching of the running system. The use of TA1, TA2.1, and TA2.2 data to inform inoculation is encouraged. TA2.3 requiring off-system connectivity or computational resources not available on-system are out of scope for the Red-C program.

**TA3 – T&E**

TA3 activities will be handled by a Government Testing & Evaluation (T&E) team. The below synopsis is included for information purposes only. Proposals will not be accepted for TA3.

The T&E Team will collect test and validation samples, run samples on hardware provided by TA1 and TA2, install Red-C firmware on TA1 and TA2 hardware, verify installed firmware algorithms are equivalent to algorithms in the deliverables, maintain and create the Red-C program website bus-watch.org. The T&E Team will be responsible for measuring and assessing the individual TAs against program metrics, as in Table 2.

*Table 2: Red-C Program Metrics*

| **Metric** | **Phase 1** Prototype |
|---|---|
| Attack detection and recovery time | Laptop PCIe[8] < 20 sec, < 5 min |
| Red-C's overhead as % of component and bus usage | Component <13%[7], Bus < 13%[6] |
| Accuracy of detection on previously unseen samples | Baseline |
| Restoration quality | Critical system function[8] is retained and the attacker's ability to exploit the same vulnerability is removed. |
| Time to implement Red-C in firmware from model on a new system | Baseline manual translation with standard development workstation |

[7] 13% is the total overhead, including instrumentation, attestation, and repair

[8] Metric will be defined by operational relevance for each bus-based system

Relevant test and validation malware samples will be collected via publicly available samples (e.g., malware for PCIe could be sourced from VirusTotal or Malpedia). Relevant samples shall represent the SOTA for current Advanced Persistent Threats for PCIe or CXL buses, including ransomware. The T&E Team will ensure malware runs exhibiting full relevant behaviors on TA1 and TA2 performers systems.

The T&E Team will create and maintain the bus-watch.org website and verify deliverable open-source; code, dataset, and algorithms following a similar framework to scikit-learn. To lower the barrier to entry for Red-C compliant firmware production, a learning/development environment called bus-watch.org will be the central Red-C community environment containing datasets, emulations, algorithms, and python code enabling experimentation and contribution. As scikit-learn enabled the development and adoption of machine learning, bus-watch.org will enable the development and adoption of Red-C compatible firmware.

The T&E Team will run test/validation samples on TA1 and TA2 hardware, collect traces, replay traces, and score TA1 and TA2 with respect to relevant metrics for the life of the program. TA2.3 strategic patches shall be installed and T&E Team tests rerun ensuring systems are inoculated to the attacks in the test and validation set.

### Schedule, Meetings, and Milestones

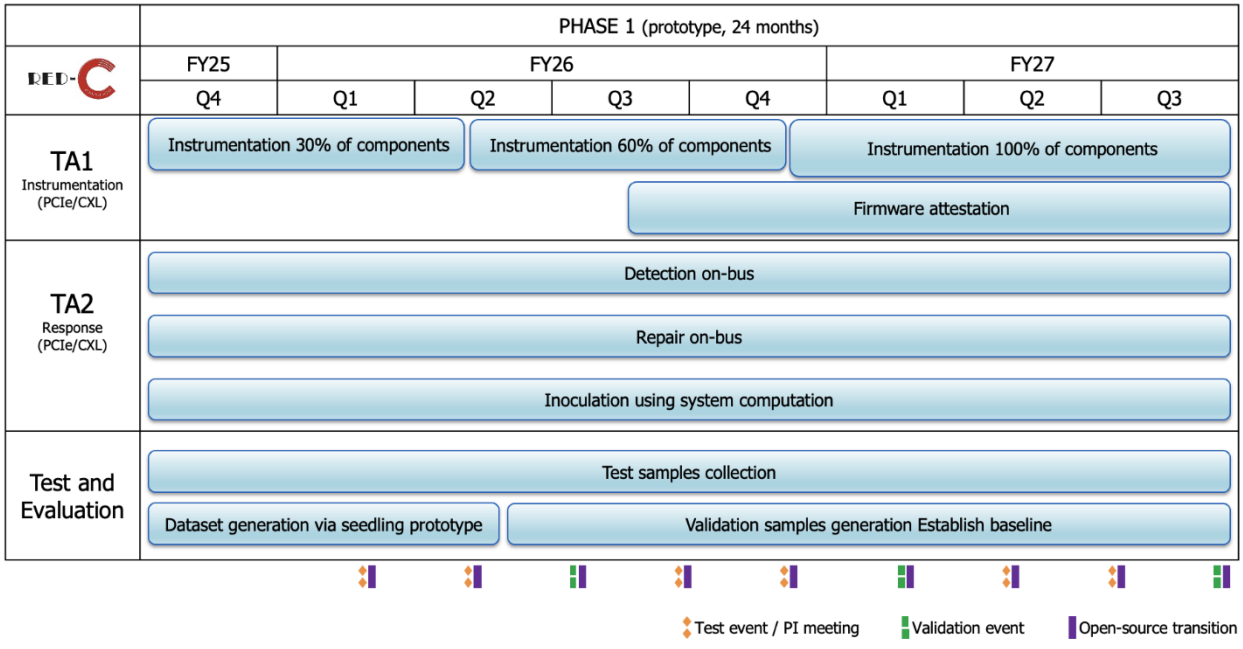



*Figure 3: Red-C Program Schedule*

As depicted in Figure 3 above, the Red-C program will consist of a single, 24-month phase with various program events throughout the program. Events will include the kickoff meeting and six combined Principal Investigator (PI) meetings/evaluation events. Proposers should plan and

budget for the attendance of appropriate and relevant personnel at each of the PI meetings and evaluation events. Relevant personnel may vary by event type; however, best practice is to assume that technical events should be attended by everyone likely to contribute to the objectives and PI meetings should be attended by everyone with significant roles in the program who could contribute to, or benefit from, the discussions at the meeting.

For budgeting purposes, assume the locations of events will be Arlington, VA. The Government also anticipates making visits to performer sites at least once every eight months, which should be budgeted for as one-day events.

## SECTION IV: 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; Firmware and Hardware Access and Capabilities; and Cost Realism.

- **Overall Scientific and Technical Merit**: The proposed technical approach is innovative, feasible, achievable, and complete. 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.
- **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.
- **Firmware and Hardware Access and Capabilities**: The proposal clearly states the proposer's access to source code and hardware and proposer's ability to repackage and reflash firmware.
- **Cost 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). It is expected that the effort will leverage all available relevant prior research in order to obtain the maximum benefit from the available funding. For efforts with a likelihood of commercial application, appropriate direct cost sharing may be a positive factor in the evaluation. DARPA recognizes that undue emphasis on cost may motivate proposers to offer low-risk ideas with minimum uncertainty and to staff the effort with junior personnel in order to be in a more competitive posture. DARPA discourages such cost strategies.

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: General Terms and Conditions.

## SECTION V: SUBMISSION INFORMATION

This announcement allows for multiple award instrument types to be awarded, to include Procurement Contracts, Cooperative Agreements, and Other Transactions for Prototype. 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.

**Proposers must review the following links:**

- **Proposer Instructions: General Terms and Conditions**: https://www.darpa.mil/work-with-us/proposer-instructions
- **Procurement Contracts**: https://www.darpa.mil/work-with-us/procurement-contracts
- **Assistance (Grants and Cooperative Agreements)**:
- **Other Transaction agreements**: https://www.darpa.mil/work-with-us/other-transaction-agreements

Full proposals are due: April 10, 2025 at 5:00 PM as stated in Section I: Overview Information. The Proposal Attachments contain specific instructions and templates that constitute a full proposal submission. Please visit Proposer Instructions: General Terms and Conditions for specific information regarding submission methods through the Broad Agency Announcement Tool (BAAT).

**Proposal Attachments:**

- Attachment 1 - Proposal Instructions and Volume I Template (Technical and Management)
- Attachment 2 - Proposal Instructions and Volume II Template (Cost)
- Attachment 3 - Proposal Summary Slide Template
- Attachment 4 - DARPA Standard Cost Proposal Spreadsheet
- Attachment 5a – Baseline Model Contract (Large Business)
- Attachment 5b – Baseline Model Contract (Small Business)
- Attachment 5c – Addendum for Circumstance-driven Clauses
- Attachment 6 – Model Cooperative Agreement
- Attachment 7 – Model Other Transaction for Prototype

## SECTION VI: 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 takes 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 shall be at the unclassified level. No CUI or classified proposals will be accepted under this solicitation.
- DARPA encourages technical solutions from all responsible sources capable of satisfying the government's needs. To ensure fair competition across the ecosystem, DARPA prohibits contractors/performers from concurrently providing Systems Engineering Technical Assistance (SETA), Advisory and Assistance Services (A&AS), or similar support services and being a technical performer, unless the DARPA Deputy Director grants a written waiver. DARPA extends this prohibition to University-Affiliated Research Centers (UARCs) and Federally Funded Research and Development Centers (FFRDCs) including National Labs, who as a result of their specialized expertise and areas of competencies, are able to accomplish integral tasks that cannot be met by government or contractor resources. Therefore, these entities are highly discouraged from proposing against this solicitation as award to a UARC or FFRDC will only be made by exception. UARCs and FFRDCs interested in this solicitation, either as a prime or a subcontractor, should contact the Agency Point of Contact (POC) listed in the Overview section prior to the proposal (or abstract) due date to discuss potential participation as part of the government team or eligibility as a technical performer.
- As of the date of publication of this solicitation, the Government expects that program goals as described herein may be met by proposers intending to perform fundamental research and does not anticipate applying publication restrictions of any kind to individual awards for fundamental research that may result from this solicitation. Notwithstanding this statement of expectation, the Government is not prohibited from considering and selecting research proposals that, while perhaps not qualifying as fundamental research under the foregoing definition, still meet the solicitation criteria for submissions. If proposals are selected for award that offer other than a fundamental research solution, the Government will either work with the proposer to modify the proposed statement of work to bring the research back into line with fundamental research or else the proposer will agree to restrictions in order to receive an award. For additional information on fundamental research, please visit Proposer Instructions: 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 http://www.darpa.mil/work-with-us/additional-baa.

- 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.

- The APEX Accelerators program, formerly known as the Procurement Technical Assistance Program (PTAP), focuses on building strong, sustainable, and resilient U.S. supply chains by assisting a wide range of businesses that pursue and perform under contracts with the DoD, other federal agencies, state and local governments, and government prime contractors. See www.apexaccelerators.us/ for more information.

  APEX Accelerators helps businesses:
  o Complete registration with a wide range of databases necessary for them to participate in the government marketplace (e.g., SAM).
  o Identify which agencies and offices may need their products or services and how to connect with buying agencies and offices.
  o Determine whether they are ready for government opportunities and how to position themselves to succeed.
  o Navigate solicitations and potential funding opportunities.
  o Receive notifications of government contract opportunities on a regular basis.
  o Network with buying officers, prime contractors, and other businesses.
  o Resolve performance issues and prepare for audit, only if the service is needed, after receiving an award.

- Project Spectrum is a nonprofit effort funded by the DoD Office of Small Business Programs to help educate the Defense Industrial Base (DIB) on compliance. Project Spectrum is vendor-neutral and available to assist businesses with their cybersecurity and compliance needs. Their mission is to improve cybersecurity readiness, resilience, and compliance for small/medium-sized businesses and the federal manufacturing supply chain. Project Spectrum events and programs will enhance awareness of cybersecurity threats within the manufacturing, research and development, and knowledge-based services sectors of the industrial base. Project Spectrum will leverage strategic partnerships within and outside of the DoD to accelerate the overall cybersecurity compliance of the DIB.

  www.projectspectrum.io is a web portal that will provide resources such as individualized dashboards, a marketplace, and Pilot Program to help accelerate cybersecurity compliance.

- 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 on-demand 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.