Reclaiming Bus-based Systems During Compromise (Red-C)
HR001125S0005
Frequently Asked Questions and Answers

Question submittals for the Red-C BAA have closed as of 5:00 PM ET on March 6, 2025. No additional questions will be accepted or answered at this time.

As of April 2, 2025

74. Q. On page 16 of the BAA, it is stated that the proposal attachments constitute a full proposal submission. However, Attachments 5a, 5b, 5c, 6, 7 seem to be related to post-award. Is it correct to assume that at this time we need to only submit Attachments 1, 2, 3, 4?

A. See answers to questions 67 and 68 for additional guidance on this topic.

73. Q. Will there be structured integration requirements or mandatory collaboration frameworks established between teams for the purpose of pairing TA1 and TA2 teams? If such pairing will occur, what process will DARPA use to ensure compatibility and integration between separately developed TA1 and TA2 components? For organizations submitting proposals only for TA1, will DARPA be pairing selected TA1 vendors with selected TA2 vendors during program execution?

A. DARPA will not pair selected TA1 vendors with selected TA2 vendors during program execution. The Red-C program website, bus-watch.org, will be the main point of collaboration. Collaboration is encouraged throughout the Red-C program.

72. Q. Should proposals include specific coordination mechanisms or interface definitions for how information will be shared between teams working on different TAs?

A. The Red-C program website, bus-watch.org, will be the main point of collaboration. Each TA should detail the expected inputs and outputs on the program website. Essentially, please anticipate that developers outside the program may use your research. Collaboration is encouraged throughout the Red-C program.

71. Q. While maintaining independent proposals for each TA, should our project schedules and technical approaches address integration points and dependencies between TA1 (Instrumentation) and TA2 (Response), particularly since TA2 will utilize Forensic Observation Data generated by TA1?

A. Both TA1 and TA2 should schedule integration time in accordance with the program schedule. Please also see the answer to question 72.

70. Q. Should we include the detailed task breakdown and project schedule/milestone charts within the DARPA Standard Cost Proposal Spreadsheet in Volume II? If so, should we include only summary information for these sections in Volume I with reference to the detailed information in the Cost Proposal Spreadsheet? If DARPA is not proposing the use of the cost spreadsheet to submit these detailed schedules and task breakdowns,

would you please consider allowing their submission as appendices to Volume I that would not count against the 25-page limit?

A. Detailed task breakdowns and project schedule/milestones charts can be included in the Volume II (Cost) submission and referenced, as appropriate, in the Volume I (Technical and Management) submission.

69. Q. I understand that the questions submittal period for this live procurement closed at 5pm EST on March 6, 2025. Is DARPA able to provide an update as to when interested vendors can expect to receive the answers to submitted inquiries?

A. The FAQ document as of March 27, 20252, will be the final FAQ document published in response to submitted inquiries.

68. Q. If redlined versions of the sample agreements should be included with our proposal, where should they go? While Volume I's Appendix A allows for us to select the reps and certs that are most applicable to our requested award vehicle and include them in the volume, there doesn't appear to be an instruction to include a redlined agreement anywhere in the volumes. Volume I instructs that "additional information not explicitly called for in Volume I […] must not be submitted with the proposal."

A. A redlined agreement may be submitted as a separate attachment from the Volume I (Technical and Management) and Volume II (Cost) submissions.

67. Q. On the SAM.gov site, there are several sample agreements included in the document list (model contract for large businesses, model contract for small businesses, and a model OTA). Are redlined versions of these sample agreements expected to be included with our proposal materials? Or are the model agreements only provided for reference and no action is expected on them for the proposal?

A. Redlined versions of the sample agreements may be submitted as a separate attachment from the Volume I (Technical and Management) and Volume II (Cost) submissions; however, this is not required by the BAA.

66. Q. We wanted to clarify if HR001125S0005 "Reclaiming Bus-based Systems During Compromise Red-C" opportunity performance period is 10/01/2025-09/30/2027 or it could be other dates.

A. Per the Section III: Funding Opportunity Description, under Schedule, Meetings, and Milestones, the Red-C program anticipates a kickoff in Quarter 4 of Fiscal Year 2025. This date is subject to change depending on the program's scientific review timeline.

65. Q. We have identified some discrepancies between the FOA and SAM documentation that we need to clarify to ensure we are preparing and submitting the correct proposal type. The FOA indicates that awards may be issued as Procurement Contracts, Cooperative Agreements, or Other Transactions for Prototypes. However, the Cost

Volume cover sheet only provides two options: Other Transaction or Procurement Contract — with no mention of Grants or Cooperative Agreements.

Additionally, the FOA does not include a link or specific instructions for submitting a Cooperative Agreement proposal. However, Attachment 6 in SAM is a model Cooperative Agreement, which adds to the confusion. When reviewing the general Cooperative Agreement instructions (which are not included in the FOA), those indicate that Cooperative Agreements should be submitted through Grants.gov.

Since this solicitation is not posted on Grants.gov, does this mean that you will only consider Procurement Contracts and Other Transactions as the applicable options for this submission?

A. Per HR001125S0005 Amendment 1, published on Sam.gov on March 15, 2025, the Red-C BAA will not consider Cooperative Agreements as a type of instrument that may be awarded.

64. Q. Planning to submit a cooperative agreement. In Attachment 1 the Representations and Certifications section only mentions procurement contracts and OT. The link under the OT also takes us to the procurement contracts reps and certs. Are the Reps and Certs required if submitting a cooperative agreement? If so, should we be using the Reps and Certs linked in the attachment (procurement reps and certs) or the Cooperative Agreement Certifications linked on DARPA's Reps and Certs page - https://www.darpa.mil/research/opportunities/reps-certs?

A. Per HR001125S0005 Amendment 1, published on Sam.gov on March 15, 2025, the Red-C BAA will not consider Cooperative Agreements as a type of instrument that may be awarded.

As of March 6, 2026

63. Q. Will DARPA please confirm if it has a preference for a HW PCIe system configuration?

A. Page 8 of the BAA states; "Red-C will only consider publicly available PCIe or CXL bus-based systems in scope". The configuration of PCIe or CXL bus-based systems are not specified.

62. Q. Will DARPA please confirm if including a public PCIe peripheral like a Raspberry Pi 5 fits in the scope of this project, or is that considered a HW solution (the goal would be to have public software/firmware and to use the compute/processing engine as a built-in cybersecurity utility processor that can monitor the bus and the other peripherals and the root-complex)?

A. Please see the BAA Table 1 for the definition of component. The system must be comprised of PCIe components.

Reclaiming Bus-based Systems During Compromise (Red-C)
HR001125S0005
Frequently Asked Questions and Answers

61. Q. Will DARPA please confirm if including a public PCIe peripheral like a programmable FPGA fits the scope of this project, or is that considered a HW solution (the goal would be to have public software/firmware and to use the FPGA as a compute/processing engine as a built-in cybersecurity utility element that can monitor the bus and other peripherals and the root-complex)?

A. Please see the BAA Table 1 for the definition of component. The system must be comprised of PCIe components.

60. Q. Will DARPA please confirm if it considers a PC (computer) with PCIe expansion slots (and populated with PCIe peripherals such as memory, SSD, NIC, GPU, etc.) as acceptable as a development and a test & evaluation platform?

A. Page 8 of the BAA states; "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)."

59. Q. Will DARPA please confirm if it prefers proposers request Firm-Fixed Price procurement contracts, with payments and cost details tied to milestones? Or is this only a preference for proposers requesting an Other Transaction for Prototypes?

A. A proposer may indicate in the proposal if there is a request for a specific award instrument. Ultimately, the Contracting Officer will make the final determination on agreement type based on what is in the best interest of the Government and the program.

58. Q. Will DARPA please confirm if the Milestone and Task tabs of the DARPA cost proposal Excel template need to be accomplished regardless of the type of Procurement Contract requested? Do they need to be accomplished if firm-fixed price milestones are requested?

A. The milestone schedule would need to be completed if fixed payable milestones are requested. The tasks tab should be completed to align with the requirement for a detailed cost breakdown that is called out in Section 7 of Attachment 1.

57. Q. The Technical and Management Volume requires extensive detailed information—including detailed technical plans, management plans, personnel qualifications, capabilities, statement of work, and schedule/milestones. Given these comprehensive requirements, would DARPA consider allowing the following two elements to be submitted as appendices that would not count against the 25-page limit:

1) The detailed task breakdown in response to Section 7 (Statement of Work)
2) The detailed project schedule and milestone charts requested in Section 8 (Schedule and Milestones)

A. These should be able to be completed within the DARPA Standard Cost Proposal Spreadsheet and would not impact the page count.

As of March 4, 2025

56. Q. With respect to the requirement "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." (BAA page 8) - is the expectation that these should be pre-existing "legacy" hardware, or is a (pre-existing) testbed that uses FPGAs to emulate the hardware (including future/in-development hardware) also acceptable?

A. The BAA states that "Proposals requiring any modification to hardware are out of scope; Red-C will not develop hardware." The hardware must exist at the time of the proposal submission.

55. Q. With respect to the requirement "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." (BAA page 8) - is that meant to say two instances of the same hardware system, or are different systems intended / expected?

A. Yes, two instances of the same hardware system - one for development and one provided to T&E team - must be included in the proposal.

54. Q. With respect to the Figure 3 timeline indicating that TA1 is expected to reach "Instrumentation 100% components" by the end of the effort and the definition of "Component" in Table 1 of the BAA, does the "Component" include things like PCIe switches, and PCIe root complex, or just the end-point components?

A. Yes, any part of the system, including the PCIe controller, may be considered a component.

53. Q. With respect to the Figure 3 timeline indicating that TA1 is expected to reach "Instrumentation 100% components" by the end of the effort and the definition of "Component" in Table 1 of the BAA - If a single bus end-point has multiple subcomponents, is it enough to instrument the end-point as a whole?

A. The BAA is not prescriptive on this, both are valid.

52. Q. With respect to the Figure 3 timeline indicating that TA1 is expected to reach "Instrumentation 100% components" by the end of the effort, do we understand correctly that the "100% components" requirement only covers the components of the particular hardware instance chosen by the performer (per "Performers shall purchase hardware instances for two system" language of the BAA)? If so, are there any expectations / requirements on how diverse that needs to be in order to be considered adequate?

A. The percentage refers to the number of components which have been instrumented to the number of components in the proposal which will be instrumented. The BAA is not prescriptive on this, the proposal should describe why their approach, and components provide coverage of the system.

51. Q. Is every TA2 proposal required to fully cover all three sub-TAs of TA2, or is it acceptable to focus on only some of them?

A. Every TA2 proposal should cover all three sub TA-s of TA2.

50. Q. Is the program's primary focus on external threats (where the malicious activity originates from one of the endpoints), while it's OK to assume that the bus hardware itself is trustworthy, or do we need to assume that the underlying bus itself is potentially compromised (e.g. a PCIe switch is malicious to begin with and could be deviating from the PCIe protocol in order to subvert our Red-C implementation)?

A. The attacker is presumed to be in the system, Red-C is reclaiming a system under active attack where one or more components are compromised.

49. Q. Is the development of custom hardware (for example, FPGAs) to monitor the bus in scope for TA1?

A. The use of existing FPGA hardware is in scope. The BAA states that "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."

48. Q. Can you please clarify to what degree performers are allowed or expected to connect additional hardware to the bus?

A. Red-C's intent is to modify the firmware of existing components on the bus. Red-C will enable zero-trust (e.g., distributed agreement) on a bus. All components on a must have a primary purpose/function and then having its firmware modified become a Red-C enabled component. Please see the BAA Table 1 for the definition of component and zero-trust.

47. Q. Is the main processor one of the components on the bus?

A. Yes, the CPU or main processor is one of the components on the bus.

46. Q. Does a component (such as a network interface card) with a driver that runs on the main processor include the driver as part of the component? Or should the driver be considered part of the main processor component?

A. Any code, firmware or software, that runs on a component is considered part of that component. For example, drivers running in an operating system on a CPU are considered part of the CPU.

45. Q. The PCIe bus is often point-to-point with a switch (not shared). In this case a component will not be able to see messages between other components. Is using multicast for FOD in scope? Are firmware modifications to the root complex to support sharing FOD on PCIe in scope?

A. Red-C is not prescriptive on the approach to securing the PCIe bus. The PCIe bus was chosen as a networked/switched bus to address the challenges this presents. In contrast a CAN bus, which is out of scope, is a broadcast architecture and presents other challenges for Red-C.

44. Q. The definition of 'Coverage of a bus' refers to 'all processes on the bus'. Do processes refer to system/user processes running on the main CPU (or other components that support multiple processes)? Or does it refer to components on the bus?

A. In the context of Red-C 'processes' refers to an abstract unit of work such as saving a file or receiving data on an open port and processing it. Red-C on the CAN bus, which is out of scope, would have processes initiated by many components.

43. Q. The definition of 'Coverage of a bus' says: 'A sufficient number of critical components which enable redundant (two or more) components' FOD generation for all processes on the bus'. Does this imply that a component should generate FOD for items (other components or processes) that are not part of the component? Or is it meant to state that there should be redundant monitoring of FOD generation?

A. The statement above is meant to state that there should be redundant FOD generation. Components' FOD generation may provide insight for other components or processes as well as themselves.

42. Q. Is it in scope for TA2 to specify the information it needs from RED-C compliant components for detection, repair and inoculation?

A. Yes, but if the specifications are not feasible then the TA2 solution may not be viable.

41. Q. Is learning benign/typical behavior (for ML or other purposes) in scope?

A. Yes, but all approach to Red-C TA2 must be robust and provide guaranties of their robustness.

40. Q. The BAA says that 'Approaches that leverage machine learning and do not prove they are robust in all use cases' are out of scope. Does this require no false positives or false negatives? Or does it require a robust defense against attacks on ML?

A. All approach to Red-C TA2 must be robust and provide guaranties of their robustness.

39. Q. Is it in scope to instrument processes on the main processor through mechanisms other than 'rewrite/modify firmware'? For example, using perf trace or similar calls as was done in the seedling dataset.

A. Any code, firmware or software, that runs on a component is considered part of that component. For example, processes running in an operating system on a CPU are considered part of the CPU. Proposals must rewrite/modify multiple components' firmware.

38. Q. Section TA2.1 refers to a 'bus-based system user'. Can you define this term? Is a process running on the main processor (that could communicate with the user of the system via a desktop user interface or an external network connection (for systems without a display) a reasonable example? Or would using IPMI be a better example?

A. User in this context means the end user or Human using the system. For example, the GPU could directly display on a monitor a message to the user (e.g., text, QR code).

37. Q: What classification level is anticipated for the project and project deliverables?

A: Red-C is an unclassified program.

36. Q: Are foreign nationals, foreign companies allowed to participate as project partners?

A: There are no restrictions placed on performer status, as Red-C is an unclassified program.

35. Q: Are green card holders allowed to participate?

A: There are no restrictions placed on performer status, as Red-C is an unclassified program.

34. Q: What is the expected review and award process timeframe anticipated?

A: DARPA will not be disclosing award timeline for Red-C

33. Q: Is there a ceiling award amount for this particular opportunity?

A: DARPA will not be disclosing the budget or project ceiling for Red-C.

32. Q: How many awards are expected?

A: DARPA will not be disclosing information on the number of awards that are anticipated or expected.

As of February 28, 2025

31. Q: We are interested in applying for this funding opportunity. The solicitation states the types of instruments that may be awarded are Procurement Contracts, Cooperative Agreements, and Other Transactions for Prototype. However, this opportunity is not showing on Grants.gov. Is this opportunity still open? How should we submit our proposal?

A: The opportunity is still open and the solicitation has been posted on SAM.gov, as opposed to grants.gov, and can be accessed via the following link: https://sam.gov/opp/6d7d9e282e31451684a0da0430d12ac5/view

30. Q: How strict is the interpretation of zero trust in the context of inoculation? If it doesn't need to be formal zero-trust for TA2.3, what are the expectations for it across the other TAs?

A: Red-C uses the following informal definition, in the BAA table 1, Zero-Trust: “Each of the components is monitoring its peers to detect, repair, and inoculate”.

29. Q: If we have an NVMe on PCIe that is thrashing around in a strange way that is not erroneous, and we force a reversion, how much of a deduction is that?

A: NVMe (NVM Express™, or Non-Volatile Memory Express) storage usage patterns may be part of a TA1 instrument. Proposals need to describe forensic density and utility of their approach.

28. Q: Does the program expect the code to build with the firmware but exist out-of-tree?

A: 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. The firmware source inspected can be in part (e.g., out-of-tree) or the full source code.

27. Q: Will we have access to the firmware we want to instrument, or is our instrumentation expected to occur on previously compiled targets?

A: As stated in the BAA, “Proposers shall clearly state their access to source code or ability to repackage firmware, access to hardware, and their ability to reflash firmware.”

As of February 12, 2025

26. Q: We'd like some clarification of side loading instrumented firmware into PCIe/CXL endpoint devices. From the proposer's day presentation and the RED-C BAA we have the understanding that hardware components are not allowed in this for security, it must all be FW based. Please clarify.

A: Red-C is an approach to securing legacy systems via firmware modification. Hardware changes are not in scope.

25. Q: Are there more datasets beyond what MITRE is hosting on their box website?

A: No, these data are a primer to provide a datapoint for state of the art in instrumenting components on a bus via firmware modification.

24. Q: For the RED-C models, does the software have to be written in python? Our understanding is that you want to host Jupyter notebooks to try things is code for modeling/simulation of CXL switches and fabrics written in other languages in scope.

A: Yes, model code should be written and packaged in a way that enables the broader research community to access and utilize it. Whenever possible, low-level languages like C should be wrapped in higher-level languages, such as Python, to facilitate greater usability and collaboration.

23. Q. If we lead a TA1 proposal, can we participate as a subawardee under another entity's proposal for TA2?

A: Yes, each proposal should be independent and specific to a TA. It should include the complete team for that specific TA.

As of February 4, 2025

22. Q: If FPGA bitstreams are considered firmware and in scope as component firmware: Given that firmware on proprietary devices can be part of a given solution, are FPGA SoC devices in scope as a PCIe/CXL CPU host device in the system?

A: FPGA bitstreams may be considered as firmware. Please see BAA table 1 for the definition of a component.

21. Q: If FPGA bitstreams are considered firmware and in scope as component firmware: Given that firmware on proprietary devices can be part of a given solution, are proprietary FPGA-based bus-connected devices, such as NICs and disk controllers in scope to include as components in the hardware system?

A: FPGA bitstreams may be considered as firmware. Please see BAA page 9 paragraph 4.

20. Q: Are FPGA bitstreams considered firmware and in scope as component firmware?

A: FPGA bitstreams may be considered as firmware.

19. Q: The solicitation specifies that proposals must address PCIe or CXL bus-based systems. Would a proposal that focuses on only one of these buses (either PCIe or CXL) be considered both fully compliant and equally competitive, or is addressing both necessary to meet the solicitation's requirements and strengthen the proposal?

A: Yes, a proposal may address either PCIe or CXL bus.

18. Q: Are there any restrictions on a company submitting or participating in multiple proposals under this solicitation, either as a prime or as a subcontractor?

A: There are no restrictions in this regard, but proposers should be able to clearly articulate that, in the event of multiple awards, adequate attention will be paid to all awards and performance on one agreement will not suffer for performance on another agreement.

17. Q: If our proposal gets accepted, would DARPA share a representative PCIe/CXL-based system design with us that we could use to validate and showcase our solution?

A: Red-c proposals must include two bus-based systems covering either PCIe or CXL. One system for testing and one for the proposer to develop on.

16. Q: If the answer to the question # 1 is yes, which hardware design language would it use - SystemC or some other language?

A: No, please refer to the BAA.

15. Q: How many awardees are expected per TA?

A: DARPA will not be disclosing information on the number of awards that are anticipated or expected.

14. Q: Please clarify if the government has any expectations on budget.

A: DARPA will not be disclosing the budget or project ceiling for Red-C.

13. Q: If a Team of performers intends to propose the program covering both TA1 & TA2. Should both of the individual TA1 & TA2 proposals be submitted as a complete team, or just from the performer's relevant to that TA?

A: Each proposal should be independent and specific to a TA. It should include the complete team for that specific TA.

12. Q: What is the project ceiling for this effort / BAA?

A: DARPA will not be disclosing the budget or project ceiling for Red-C.

11. Q: How do you anticipate FFRDC institutions participating in this effort?

A: Please each out to the redc@darpa.mil for individual discussions

10. Q: There was a note about T/E team on one of the slides. Curious if there is gov team in that space. Related to that, are you envisioning that the program's instrumentation and repair capabilities will target components with source code and build environments or just plain old binary patching?

A: MITRE is the T and E team for Red-C. Either or both approaches are valid investigative paths.

9. Q: Mr. McShea's presentation seemed to indicate open-source transition as the goal - would source available commercial software that requires a reasonable licensing cost for commercial use be acceptable and competitive? What is the preferred way for a vendor that needs a reasonable amount of licensing revenue to sustain the technology to participate?

A: Algorithms developed under Red-C, datasets and models must be open sourced, all else can be proprietary.

8. Q: Given the citation of DARPA GARD and the vulnerabilities of AI/ML, does Red-C discourage ML in any or all of its components?

A: Solutions to Red-C should have robustness guarantee by construction.

7. Q: Are classified proposal responses anticipated?

A: No.

6. Q: Are any organizational eligibility limitations anticipated?

A: No.

5. Q: Is RED-C limited to just PCIe and CXL buses, or is CAN bus included as well?

A: Red-C is limited to just PCIe and CXL buses.

4. Q: What would the process to be part of the TAV team for this effort? Any limitations?

A: We are not accepting proposals for test and evaluation team

Reclaiming Bus-based Systems During Compromise (Red-C)
HR001125S0005
Frequently Asked Questions and Answers

3. Q: Is there an assumption that firmware instrumentation is to be done with components' source code or expecting direct modification of firmware's binary/image?

A: Either way is acceptable.

2. Q: Are you interested in solving this problem at only firmware level? Or, would you be interested in exploring cybersecurity problem at RTL (chip) level?

A: We are interested in the PCIe and CXL bus level.

1. Q: Is there interest within the Red-C program to understand adversary attack techniques of bus protocols, or to obtain relevant datasets for testing?

A: T&E team will be responsible for doing this.