Q43: Where are the AMP proposer day slides posted?
A43: The AMP proposer day slides can be found at the following link:
https://www.darpa.mil/attachments/AMPProposerDaySlides_Bratus_Final_with_QA.pdf

Q42: Is the scope of the AMP program limited to security or is there a relationship between security and safety?
A42: The focus is primarily on security. Please refer to the BAA for some discussion in related subjects.

Q41: We were potentially interested in submitting a TA1 abstract but also considering options as a subcontractor for a TA3 abstract. Will we be able to submit as a Prime on a TA1 submission and participate on a TA3 submission as a sub? If there is a restriction, is it only applied on the full proposal or on the abstract phase also?
A41: Per the BAA, a proposer submitting a proposal to TA1 and another to TA2 may be selected to perform on both TAs. However, selected TA3 performers cannot perform on any other TA. Proposers who consider submissions to, e.g., both TA1 and TA3 can take advantage of the optional abstract phase to receive feedback.

Q40: Page 12 of the BAA mentioned "combine commodity cellular modem with access to the vehicle's systems". Should we assume that binary code would also include cellular code and not just the embedded code for mission critical functions such as engine, brake control code? And security protection needs to extend also to the cellular code?
A40: No such assumption is expected. Page 12 discusses an exemplary use case for TA3 challenges, but does not limit TA3 to this exemplary case. See also Q34.

Q39: For human-in-the-loop (Phase 1), is it correct to assume that the human would be able to provide some limited information to the tool about the embedded systems or the application that the given binary code is intended for?
A39: Such assumption would be in scope, but must reflect standard industry practices and patching use cases.
Q38: Is it correct to assume that these codes are probably for older processor architectures? Would it be in scope of the BAA if we only target architectures that we believe are applicable to mission critical code?

A38: The BAA calls for technological breakthroughs in assured patching of binaries across a variety of mission-critical platforms. Strong proposals are not expected to have essential dependencies on a particular architecture.

Q37: Code with lost source or documentation are likely to be very old code. How far back in time do we need to plan for in the proposal? 20 years, 40 years?

A37: The BAA does not make limiting assumptions about the age of systems for which the ability to fully rebuild their software binaries is unavailable. Strong proposals are expected to offer technological breakthroughs without essential dependencies on particular architectures.

Q36: Will there be classified information during execution?

A36: No. No CTI or classified information will be used.

Q35: Are TA3 providers able to provide a virtualized image containing binary/firmware, as opposed to providing physical devices for phase 1?

A35: See A34. A progression from virtualized challenges to physical devices is expected.

Q34: Are TA3 providers free to offer up different platforms other than heavy vehicle?

A34: Yes. We do not limit use cases other than by requiring that they contain no CTI. CTI is out of scope.

Q33: Will TA3 create patches in a format specified by performers, or just source?

A33: TA3 challenges will approximate a variety of structured ways in which mitigation strategies are described; source patches will be expected to constitute the base case.

Q32: Are approaches targeting a single compiler family but covering a range of options acceptable?

A32: Strong proposals will cover a broad range of industry development practices.

Q31: What source languages and compilers should be supported?

A31: Assume common industry development practices for embedded
devices. Addressing C is anticipated.

Q30: Will there be different perspectives in TA1 and TA2? Will they be reconciled?
   A30: The BAA is not prescriptive with regards to particular designs. Designs will be expected to reflect and address practical industry concerns. See also Q29.

Q29: How high level will the IRs be?
   A29: Design of IRs and interaction between IRs is an open in-scope research question for the proposer.

Q28: What are we to assume about security mechanisms built into the binary, such as signatures, periodic integrity checks? Is it part of the program to overrun thee or are thee known as the baseline?
   A28: We will not assume the need to overcome or circumvent security mechanisms.

Q27: May the TA2 proof-guided testing and non-interference proofs assume the semantics of the binary ISA is correct? That is, binary instructions do what they should do, without “weird machine” or undocumented behavior?
   A27: Generally, yes. The platforms are expected to be well-understood, and their unusual behaviors sparse and understood at usual industry levels.

Q26: Are any particular source languages, such as C, C++, and ADA, emphasized or deemphasized?
   A26: Common industry practices, such as C, are emphasized.

Q25: Are proposals to multiple TAs encouraged or discouraged? Are cross-references or dependencies between TA1 and TA2 proposals encouraged or discouraged?
   A25: Multiple proposals are welcome to TA1 and TA2. Proposals may cross-reference, but will be evaluated on their individual stand-alone technical merit.

Q24: How important are usable prototypes, as products of this effort?
   A24: Very important.

Q23: What is the target architecture, e.g. ARM? 32-bit?
   A23: Proposals are not limited to any particular architecture but must reflect common
industry practice.

Q22: Can we assume that the patched code has any unit tests and/or pseudo code descriptions of the nature of the patch?

A22: Both assumptions are plausible, and strong proposals will discuss ways to accommodate such information. However, strong proposals will also discuss ways to compensate for lack of unit tests.

Q21: Do you anticipate or have required down selects at the end of phase 2?

A21: The BAA does not specify down selects, however, please refer to page 8 of the BAA for the description of the phased structure of the program.

Q20: How are patches specified? Any formalism assumed?

A20: No specific formalism is assumed for patches. Proposals should address common industry practices. Slide 17 of the posted Proposers’ Day slides outlines a baseline case. (https://www.darpa.mil/attachments/AMPProposerDaySlides_Bratus_Final_with_QA.pdf)

Q19: Are specific languages required, preferred, prohibited?

A19: No languages are prohibited. Proposers are expected to address common industry practices and languages, such as C.

Q18: Is binary rewriting out of scope (it spans TA1 and TA2)?

A18: All techniques that produce strong assurance in the time frames discussed in the BAA are in scope.

Q17: Is the decompilation of binaries to understand violations of proven-aware, control-theoretic violations of safety constraints in scope?

A17: Yes, but the focus of the program is primarily on security patches.

Q16: What is the desired TRL level for each phase?

A16: The program is expected to make substantial fundamental research advances and produce prototypes. Higher TRL levels are encouraged to enable transition.

Q15: What certification process for assurance?
A15: Strong proposals will address common industry procedures used for certification.

Q14: Whereas TA1 concerns are assured recompilation, TA1 doesn’t include assured decompilation. Are assurance arguments on semantical equivalence of interest for TA1?
   A14: Yes. Significant fundamental research advances are expected in TA1.

Q13: If I am a TA1 proposer, do I need to talk to TA2 proposers to determine my output format to ensure interoperability? Same question, if I am a TA2 proposer.
   A13: Proposals will be evaluated on their individual stand-alone technical merit. However, TA1 and TA2 interaction is strongly encouraged, as per the BAA. Development of novel technologies for enabling TA1 and TA2 interaction is encouraged.

Q12: Will there be or could there be multiple devices for an evaluation, and therefore, multiple ground truth?
   A12: Yes, multiple challenges of increasing complexity and “trickiness” are expected.

Q11: What is the source of ground truth for the accuracy and human effort metrics? TA3?
   A11: Yes, TA3 will propose challenges that will include source code used as the ground truth but not fully shared with performers.

Q10: Does the program seek TA1 proposals that focus on the breadth of systems, e.g. functional language program binaries, very old platforms (non-8-bit, non-ASCII)?
   A10: Yes, breadth is encouraged. However, the common industry use cases and practices need to be addressed.

Q9: I suspect that industry is continuing to make new binaries that will suffer/cause the problem you want to solve. What best practices do you recommend to mitigate these future problems?
   A9: The program solicits proposals for solutions at this time. It makes no recommendations.

Q8: Can you provide some concrete decompilation goals?
   A8: Please refer to the BAA examples. Strong proposals will address a variety of realistic goals common for the industry.
Q7: Can we assume we can do in-production fault-injection?
   A7: TA3 will be expected to accomplish this.

Q6: Can we assume we can monitor applications at runtime (e.g. some light weight recording, etc.).
   A6: All necessary practical analyses are in scope.

Q5: Is automated testing and validation of patched binaries in scope for TA2?
   A5: Yes.

Q4: Can you give an example of a format that would be acceptable for TA2 proofs? Math?
   A4: Any format suitable for industry-standard procedures for certification guided by practice.

Q3: The metrics table refers to accuracy relative to ground truth for TA1. What constitutes ground truth and how will accuracy be measured?
   A3: Ground truth in challenges will include known source code, produced by TA3 (but not shared fully with the performers). Accuracy metrics will develop during the program through input from the SMEs and practical suitability of results for the use cases and challenges.

Q2: Can TA3 approach be fully virtualized or is real hardware expected?
   A2: TA3 may start with virtualized systems in Phase 1, but is expected to create real hardware challenges later in the program.

Q1: Looking forward, wouldn’t we want to produce the information necessary for micropatching during initial compilation? Is that in-scope?
   A1: Yes, this would be in scope. However, a proposed solution should not assume availability of such information for the core case.