

**Military Network Protocol (MNP) Program DARPA-BAA-09-11
Solicitation
Questions and Answers**

The following BAA questions and answers are provided.

1. Question: Will the MNP system be declassified at the end of the program?
Answer: The intent is that the final MNP product suite be moved from classified to ITAR restricted at the end of the program.
2. Question: How will you get classified protocols through the standards process?
Answer: We will address the possibility of changing the classification early in the program. Additionally, it is possible to have different versions of the software, one for military use, and another for commercial.
3. Question: How can a commercial networking company be involved if “all implementation software” is classified?
Answer: They can be involved if they want to do the work.
4. Question: Does testing need to address existing military systems (*e.g.*, GCCS, etc.)?
Answer: Optional: The military mostly runs TCP/IP and is basically commercial anyway. There will not be government furnished equipment. Do not jeopardize your program execution by relying on military equipment.
5. Question: How do you want test performer pricing broken down?
Answer: Level of effort, labor categories and labor rates.
6. Question: Should the product work on Internet Protocol Version 4 (IPv4) or Internet Protocol Version 6 (IPv6) or both?
Answer: Both by Phase 3.
7. Question: HAIPE Encryption Architecture. Are you assuming a HAIPE based environment or ignoring HAIPE-like encryption?
Answer: MNP needs to work in a military environment, through link encryptors, and with either a black core or a conventional plain-text core. A black core will understandably affect MNP capabilities for traceback, etc. Performance testing will be done on a conventional core.
8. Question: Lines between classified and unclassified research. University X has a working technology that they have evaluated, tested, and classified. We want to use it. Isn't it classified already?
Answer: No. First, you will likely make some changes. Also, it will not perform identically in MNP and on a large network as it does in the university lab. You do not need to tell them about either the changes or the actual performance.
9. Question: Can uncleared people work on the system design or analyze potential vulnerabilities?

Answer: Yes.

10. Question: SSL and encryption. Page 8 of the BAA suggests Type II encryption of MNP specific data (*e.g.*, attribution) is within scope. Correct?
Answer: Correct. Type I encryption is also acceptable if it is cheap and its incorporation does not require NSA hardware certification. However, the likelihood of anyone having Type I encryption equipment that does not require NSA certification and is inexpensive is very low. If you do meet these criteria, please explain how you do this fully in your proposal.
11. Question: If we propose to satisfy the program requirements with off-the-shelf hardware components, is a vendor supplier agreement sufficient for a manufacturing partner?
Answer: Yes, but you must provide in your proposal how X number of boxes will be made by the end of the three year period and how you will produce large numbers of devices in the future.
12. Question: Regarding metrics, how would a CONOPS make use of 32 priority levels?
Answer: We want 32 levels or more, we will let the military figure out how to best utilize them.
13. Question: How many trusted network controllers are being considered for MNP?
Answer: Disclose in your proposal how many trusted controllers will be used. Trusted controllers should be kept to a minimum. However, there should never be a single point of failure. If you look at this from a military operation perspective, there should be 3–4 places in a division where a user with the correct credentials should be able to reconfigure the network.
14. Question: Is there a network traffic profile (or multiple profiles) that will be provided by the government?
Answer: No.
15. Question: Is the MNP effort required to address Byzantine failures of network controllers (*e.g.*, arbitrary misbehavior of network controllers)?
Answer: It is not required.
16. Question: How many ports (of different line speeds) must be supported by the network controller for each phase of the program?
Answer: Four ports.
17. Question: Metrics for time to distribute C2 instructions and fetching configuration file from another network controller—this depends on available bandwidth. Do these metrics have an implicit bandwidth assumption?
Answer: No.
18. Question: Testing metrics seem to be focused on relatively high bandwidth. Military networks tend to have low bandwidth. Considering MLPP and QOS focus mentioned,

protocols that are best for high bandwidth may not be best for low bandwidth. Would you require testing at low bandwidth?

Answer: Yes.

19. Question: Are you interested one conservative approach and some experimental ones?

Answer: We will fund the best ideas. Innovation is great but we need to meet the program's metrics as well. The two are not mutually exclusive.