

1. The following questions were submitted in response to this RWP. The Government's responses are provided below:

| AMENDMENT 0002 | | |
|----------------|---|--|
| Number | Question | Answer |
| 1 | Will the Government please confirm the Period of Performance for Phase 1 is 4 months in duration, and Phase 2 is 12 months in duration for a total of 16 months of performance? | Confirmed. |
| 2 | Can the Government specify the contract type (T&M, FFP, CPFF, etc) for the ROM? | FFP. |
| 3 | Can the Government confirm that a Cover Page may be included in addition to a Cover Sheet, and that the Cover Page will not count against page count? | Confirmed. |
| 4 | Will Government confirm that the Table of Contents can be organized at the beginning of the Technical Volume immediately after the Cover Sheet and Cover Page? | Confirmed. |
| 5 | Can the Government confirm that the updates every two months begins after the initial report? | In Phase 2 (RWP Table 3, pg 20) of the Performance Acceptance milestone after the initial report (8 th month mark) updates are due every two months thereafter. |
| 6 | Can the Government clarify the 3-month update cadence and whether that begins at start of PoP or following initial delivery? | In Phase 2 (RWP Table 3, pg 20) of the full PKI ecosystem demonstration updates are due every 3 months after initial delivery (8 th month mark). |
| 7 | Can the Government specify the contract type (T&M, FFP, CPFF, etc) for the ROM? | FFP. |
| 8 | Would the Government please confirm the Project Number. The page headers read, "Project Number: DISA-OTA-22-R-QRC"; however, in the table below on the same page it reads, "DISA-OTA-22-9-QRC". | The Project Number is DISA-OTA-22-9-QRC. RWP Amendment 002 corrects project number in header. |
| 9 | To assist, plan and forecast resources for the presentation, can the government share any details on the oral presentation? | Oral presentations will be held virtually via MS Team. The date and time TBD. |

| | | |
|----|--|---|
| | (Virtual/Physical? Location? Presentation time?) | |
| 10 | Given several of the NIST post quantum algorithms have been breached (SIKE / Crystals Kyber), would DISA be willing to look at alternative algorithms as part of this OTA or algorithms that would strengthen these NIST approved algorithms described in the OTA? | At this time DISA is interested in NIST Selected Algorithms 2022 (https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms-2022) and algorithms in NIST Round 4 Submissions (https://csrc.nist.gov/projects/post-quantum-cryptography/round-4-submissions) |
| 11 | Can DISA please share if the Test Harness needs to be in a government certified test environment or if for purposes of demo it can be on public cloud infrastructure (Google, Microsoft or AWS)? | The Test harness can be developed in the vendor's environment for demo purposes, but ultimately the solution needs to be delivered to the Government for installation in a government-controlled testing environment. The solution will not require an Authorization to Operate at the time of delivery. |
| 12 | Will the government extend the due date of Phase 1 white papers to September 30th, 2022 to allow time for firms to collaborate with industry which will support a comprehensive innovative technical solution. | No extensions will be granted. |
| 13 | In Section 3.4.2 the government States "The work to be performed under this prototype OTA is up to the Secret level. Therefore, the vendor must have an interim or final Secret Facility Clearance from the Defense Counterintelligence and Security Agency at time of White Paper submission." Is it permissible for a subcontractor to hold the Secret Facility Clearance at time of white paper submission to comply with this requirement? | Yes. |
| 14 | Will the government please clarify if Traditional defense contractors are required to subcontract a specific percentage of scope with Nontraditional defense contractors? | A nontraditional defense contract must perform a significant portion of the work. If a traditional defense contractor does not propose to use a NDC to perform a significant portion of the work, the traditional contractor must enter into a 1/3 cost share arrangement with the Government. |

| | | |
|-----------------------|--|---|
| 15 | Will the government facilitate an industry day or matchmaking sessions with interested vendors as this is a similar practice with OTAs? | No. |
| 16 | Will the government facilitate one on one discussions with the Program Management team for this effort in addition to the formal Q&A? | No. |
| AMENDMENT 0003 | | |
| 17. | The patent owner's statement in Section 2.3.2 states as follows: I, [insert full name], of [insert full postal address], am the owner or authorized representative of the owner [print full name, if different than the signer] of the following patent(s) and/or patent application(s): [enumerate], and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as [insert name of cryptosystem] is selected for the DoD prototype, in consideration of its evaluation and selection, a non-exclusive license for the purpose of implementing standards or algorithms [check one]:" Can the government please define "interested party" for the purposes of this paragraph or otherwise clarify that submitters are permitted to define "interested party" in their white paper submissions? | Note: For the purpose of this Prototype OTA RWP, an interested party is any party that needs to have access to the solution as part of its performance. |
| 18. | Will the government please clarify if for "Task 1. Provide a QRC-Enabled Certificate Authority" the anticipated solution is Software, hardware, or a combined software and hardware root of trust? | The Government is looking for Industry to propose a solution. |
| 19. | In Section 3.4.2 the government States "The work to be performed under this prototype OTA is up to the Secret level. Therefore, the vendor must have an interim or final Secret Facility Clearance from the Defense | See response to Question 13. |

| | | |
|-----|--|--|
| | Counterintelligence and Security Agency at time of White Paper submission.” Is it permissible for a subcontractor to hold the Secret Facility Clearance at time of white paper submission to comply with this requirement? | |
| 20. | How does the Government define subvendor? Does this include OEMs and resellers, or is this limited to subcontractors? | Note: for the purposes of the OTA, a subvendor is defined as any vendor that has a subcontract relationship with the prime vendor. By providing the required statements/agreements/disclosures under this section, a vendor confirms that they will be able to deliver the necessary products and services (including, but not limited to Original Equipment Manufacturers (OEMs) and resellers) that are in compliances with the outlined requirements. |
| 21. | Is it acceptable to redline the provided disclosure statements, or would the Government deem that as non-compliant? | Redlines are not allowed. Disclosures are to be completed in full. |
| 22. | Is the Government amenable to defining “interested party” as included on Patent Owner and Reference Owner Statements, 2.3.2 and 2.3.3 respectively. | See answer to question 18. |
| 23. | Does the Government expect Submitter Statements to be submitted by OEMs and Resellers? | Per RWP 2.3.1, Submitter Statement is required by each participant (prime vendor and each subvendor). |
| 24. | Is the Government amenable to including the language below for further clarification, “For the avoidance of doubt, any solutions developed by the vendor separate from this OTA that may have applicability to a modified cryptosystem solution specification will be subject to a new agreement between the government and the vendor.” | No, the current RWP language remains. |
| 25. | Is the Government amenable to including a clarifying statement | No, the current RWP language remains. |

| | | |
|-----------------------|---|---|
| | regarding IP developed separate from the OTA? | |
| 26. | Is the Government amenable to inserting “solely” immediately before the terms “for the purposes of the evaluation process.” This creates a defined and limited license within the grant statement. | No, the current RWP language remains. The intent is inherent in the current wording. |
| 27. | Does it meet the security requirement to have a sub be the holder of the FCL or must the prime vendor be the FCL holder? Can you please elaborate on the FCL requirement? | See response to question 13. |
| 28. | DISA has a publicly available list of vendor questions which contain a question inferring that Kyber is broken. Please provide any additional information that you can to the response? | At this time DISA is interested in NIST Selected Algorithms 2022 (https://csrc.nist.gov/projects/postquantum-cryptography/selected-algorithms-2022) and algorithms in NIST Round 4 Submissions (https://csrc.nist.gov/projects/postquantum-cryptography/round-4-submissions) |
| 29. | NSA released the Commercial National Security Algorithm Suite 2.0 that does not recommend hybrid (classical/quantum safe) migration. How does this impact Task 6? | NSA chose algorithms selected for standardization by NIST. Task 6 is using these algorithms as well as algorithms in NIST Round 4 submissions. NSA FAQ states “NSA does recommend limited use of pre-standardized or non-FIPS-validated CNSA 2.0 algorithms and modules in research settings to prepare for the transition” |
| 30. | DISA has requested secure SMIME/EMAIL capabilities. Should the ecosystem capabilities be email client or email gateway based ? | The Government is looking for Industry to propose a solution. |
| AMENDMENT 0004 | | |
| 31. | Section 3.4.2 states “All personnel performing on or supporting work on this OTA in any capacity shall be U.S. citizens.” If a company intended to present a technology as part of their response from a company comprised primarily of 2nd and 3rd Party Nationals, what | Only United States company products with United States citizens supporting the solution are authorized for responses to the RWP. |

| | | |
|-----|---|---|
| | guidance can the Government provide on how to proceed with a vendor's inclusion of that company? | |
| 32. | Section 2.3.1 requires a statement concerning whether the cryptosystem, standards, or algorithms are covered by U.S. or foreign patents or pending patent applications, or whether the submitter does not hold nor intends to hold such patents or patent applications. However, Section 2.3.1 does not address the scenario where a submitter does not presently hold a patent but intends to submit a patent application in the future that would cover the cryptosystem, standards, or algorithms. Please clarify how offerors should respond to Section 2.3.1 in this scenario. | The Government has determined that the current RWP language sufficiently addresses situations where the vendor does not currently and does not intend to hold a patent or patent applications with a claim for the future. The inherent language is applicable to cover current and future patent holdings. |