Quantum Resistant Cryptography Prototype
DISA-OTA-19-R-Quantum

#	Reference	Questions	Government Response
1	RWP 3.4.1	It is unclear how the last two bullets are applicable to Quantum-Resistance Cryptography. - Demonstrate mobile implementation suitable for 5-10 km link distances; - Ability to support classical communication channel via Radio Frequency (RF) or optical.	The Government has removed the bullets/requirements and provide additional clarification within section 3.4.1.
2	RWP 3.4.2	The following three bulleted items would seem to only have application for QKD. - Support same key generation rate as the original decoy state BB84 Quantum Key Distribution (QKD), E91 methods/protocols and other cryptography standards; - Allow for Continuous-Variable (CV) QKD encoded onto the amplitude and phase quadratures of a coherent laser, and methodology for measurement; - Detect manipulation based attacks such as, but not limited to: (a) Basis-Dependent (Control Attacks) – Perform Intercept-Resend on quantum channel and then hide the disturbance by blinding all signals measured in a different basis. (b) State-Dependent (Suppression Attacks) – Blind all detector results except for one pre-chosen state that is chosen uniformly at random for each signal. (e.g., the detector dead-time attack).	The Government has removed the bullets/requirements and provide additional clarification within section 3.4.2.
3	RWP 3.4.1	The RWP states the vendor's technical approach should "Demonstrate mobile implementation suitable for 5-10 km link distances." - In order to respond as realistically as possible, please advise if DISA has preference as to what should be demonstrated within 5-10 km? For example, radios, cell phones, etc.	The Government has removed this requirements. See updates in section 3.4.1.

4	RWP 3.4.1	The RWP states the vendor's technical approach should reflect an "Ability to support classical communication channel via Radio Frequency (RF) or optical." - Is DISA looking for a blanket RF or a targeted RF? Will DISA be providing specific parameters (payload buffer size, data, voice, video, etc.)?	The Government does not have a pre-defined blanketed or targeted Radio Frequency (RF), or specific parameter (e.g., payload buffer size, data, etc.) for the OTA prototype. The vendor may propose specific parameters and communication channels relevant to practical implementations.
5	RWP 3.4.2	The RWP states the vendor's security approach should "Allow for Continuous-Variable (CV) QKD encoded onto the amplitude and phase quadratures of a coherent laser, and methodology for measurement." - Is DISA requesting transmission (amplitude and phase quadratures of a coherent laser) measurement against a line of sight, radio frequency, guided munitions?	The Government has removed this requirement. See updates in section 3.4.2.
6	RWP 3.4.2	The RWP reflects five target security strengths ranging from "128 bits classical security / 64 bits quantum security" to "256 bits classical security / 128 bits quantum security." - Does DISA have a defined cubic test range that they wish to use?	The Government has updated this requirement and removed the 128 bit requirement. Preliminary computational resources should be measured using a variety of metrics, such as the number of classical elementary operations, quantum circuit size and consider realistic limitations on circuit depth (e.g. 240 to 280 logical gates). The Government has defined the following preliminary ranges: • Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for collision search on a 256-bit hash function (e.g. SHA256/ SHA3-256); • Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 192-bit key (e.g. AES192); • Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for collision search on a 384-bit hash function (e.g. SHA384/ SHA3-384);

			• Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 256-bit key (e.g. AES 256). Any attack must require computational resources comparable to or greater than the stated threshold above, with respect to all metrics that is deemed by the Government to be potentially relevant to practical security.
7	RWP 3.4.2	The RWP states the vendor's security approach should "Detect manipulation based attacks such as, but not limited to: a) Basis-Dependent (Control Attacks) – Perform Intercept-Resend on quantum channel and then hide the disturbance by blinding all signals measured in a different basis. b) State-Dependent (Suppression Attacks) – Blind all detector results except for one pre-chosen state that is chosen uniformly at random for each signal. (e.g., the detector dead-time attack)." Does DISA have a defined quantum-based attack vector for out of phase signal degradation that they wish offerors to understand?	The Government has removed this requirement. See updates in section 3.4.2.
8	RWP 5.2.1	The RWP states "data be 'conspicuously and legibly' marked with a protective legend that identifies the...contractor's name and address." - Is it DISA's intent that every page of an offerors submittal include the full company address in the header or footer?	No, only the cover pages is required to have the Company Name, and Point of Contact (POC) address. The Company name and address are not required on every page of an offerors submission. However, all pages should be marked accordingly to the data submitted and include the following statement within the header/footer as required: *Use or disclosure of data contained on this sheet is subject to restriction"* on the title page of any restricted data sheets. See section 5.2.1 of the RWP for additional details.
9	RWP 2.3.1, 2.3.2, 2.3.3, 2.4	Are Sub-Vendors/Consultant Labor required to affirm through signature this section, or is the Prime Vendor the only required signature?	The selected vendor will be the single entity who the Government holds accountable via a legally binding OTA agreement, therefore any sub-vendors or consultant labors are not required to sign or submit an Intellectual Property Statement, Agreements, or

			Disclosures. The selected vendor will be held liable and will expect that the selected vendor already have any required team agreements, data rights, etc. completed and in place at the time of negations.
10	RWP 3.4.1	In this section, bullet 3 the term 'quantum cryptography' is used, but the implication is 'post-quantum cryptography'. Was the term 'post-quantum cryptography' intended here?	The Government has reworded and removed requirements listed in section 3.4.1.
11	RWP 3.4.1	In this section, bullet 4 - Will DISA provide further detail on protocol information (which protocols) requirements?	The prototype will be required to address various protocols such as Public Key infrastructure (PKI), Internet Protocol Security (IPsec), the Transport Layer Security protocol (TLS), Secure/Multipart Internet Mail Extensions (S/MIME), Kerberos, Over-the-Air Rekeying (OTAR), Domain Name System Security Extensions (DNSSEC), Encrypted File Systems and the Secure Shell (SSH).
12	RWP 3.4.1 & 3.4.2	In Section 3.4.1 Bullet 6 & 7, plus Section 3.4.2 SECURITY, p. 11 of the RWP, the second, third, and 7th bullets refer to QKD systems. - Should the design of the Quantum-Resistant (QR) Cryptography prototype of interest to this OTA include Quantum Key Distribution (QKD) techniques or focus exclusively on QR Cryptography techniques? - Should the analysis of the Quantum-Resistant Cryptography prototype of interest to this OTA consider current state-of-the-art QKD techniques as a comparison system?	The Government has removed this requirement. See updates in section 3.4.1 and 3.4.2.
13	General	Will DISA permit offsite lab / remote work to be completed for this project?	To protect against seizure and improper use by non-United States (U.S.) persons and government entities, all data stored and processed by/for the DoD must reside in a facility under the exclusive legal jurisdiction of the U.S. Specific work location will be determined during negations with the selected vendor. Work may be performed on-site, at all CONUS and OCONUS Government facilities or at the contractor's facility, sub-contractor facility, supplier, or other designated locations (e.g., corporate, 3rd party, or subcontractor). For any contractor/sub-contractor facility, supplier, or other designated locations (e.g., corporate, 3rd party, or subcontractor)

			that are used to performance or meet requirements, the contractor shall provide the Government with the following detailed information: • Facility Name • Point of Contact • Description of Services/Data Provide at the location • Geographic Location and Address If a proposed solution required access or storage of DoD data or integration with supporting DoD Infrastructure Components (e.g., DoD PKI/PKE), the vendors will be required to meet the personnel and information impact level requirements outlined within the DoD Cloud Computing Security Requirements Guide.
14	General	Are there protocols in addition to TLS that a prototype should address?	See question # 11 for additional details on which protocols will be required.
15	RWP 4.2	Section 4.2 states the intent to award "one (1) prototype OTA." The field of Quantum Cryptography (e.g., Quantum Key Distribution (QKD), quantum resistant algorithms, Quantum Random Number Generators (QRNG), various protocols/algorithms, optical versus free space implementations, etc.) – from an operational deployment perspective – is still in very early stages with many areas of research and development. These are experiencing dynamic change. We suggest it may be in the Government's best interest to consider multiple awards that would afford the Government the opportunity to assess different approaches to the problem statement articulated in section 1.2.	This is a comment, not a question. No response from the Government needed.
16	RWP 3.4.1	Section 3.4.1, sixth bullet. Can the Government clarify the mobile implementation? Does this bullet apply to mobile endpoints or is the intent to explore fixed mobile scenarios?	The Government has removed this requirement. See updates in section 3.4.1.
17	RWP 2.3.2	States that- "….the owner or authorized representative of the owner…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	The cryptosystem should include all of the hardware products and any system components required for the standard or algorithms to be implemented. For example a vendor could have a cryptosystem called "Pretty Pink Pony" which includes all of the hardware

		[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..." - Does the "implementing standards or algorithms" cover hardware products and hardware systems for implementation of the cryptosystem or only the algorithms/standards to implement the cryptosystem?	products and any required system applications for their algorithm name "Funny Donkey" to run on.
18	RWP 2.3.2	The language - "under reasonable terms and conditions that are demonstrably free of any unfair discrimination…" for the non-exclusive license. Who defines the "reasonable terms and conditions"? Is there a negotiation process for this?	The Government will issue a Request for Project Proposals (RFPP) to the selected vendor. After the receipt of the RFPPs, the Government will conduct an evaluation to ensure it meets the requirements. The next step will be to invite the vendor to meet with the Government in order to engage in negotiations. The Government will provide an initial model OTA to the selected vendor, which will be the Government's opening position for negotiations. Using a collaborative process, the Government and the vendor will develop a detailed work statement, negotiate terms and conditions, agree on milestones, deliverables, and negotiate final price. Once complete and all parties are in agreement, the Government will award a prototype OTA to the selected vendor. In the event the Government is unable to reach an agreement with the initial selectee, the Government may re-evaluate White Paper responses and make another selection.
19	RWP 2.3.3	Can DISA provide examples of reasonable terms and condition? Additionally, can DISA provide examples of reasonable royalties?	Reasonable terms and conditions are specific to a vendor proposed solutions and can vary based on payment requirements, price variation, penalties, etc. All terms and conditions will be finalized during negations and included within the final Request for Project Proposal (FRPP). Royalties can also be specific to a vendors proposed solution and can vary depending upon ownership of algorithm, hardware, etc. Royalties are payments of various types to owners of property for use of that property. Royalties usually deal with payments for the right to use intellectual property, like copyrights, patents, and trademarks.

20	RWP 2.3.2	How will the OTA awardee be compensated going forward? If the Government has the right to modify the specifications, will the awardee be boxed out of future revenue?	The selected vendor will obtain payment based on agreed milestones, deliverables, etc. that are defined during the negotiation phase. All required modification to any requirements, price, terms and conditions will be finalized during negations and included within the OTA agreement. The selected will not be excluded from bidding on any follow-on production contract. See questions # 18 and the RWP section 4.1 and 4.2 for additional details on the Request for Project Proposal, negotiation phase, and the follow-on production contract information.
21	RWP 2.3.2	Who does DISA anticipate to be the interested parties under Section 2.3.2 to whom the awardee will have to license its patents?	Interested parties could be, but are not limited to other DoD Organizations or Intel Communities who currently have ongoing research and development efforts for Quantum Resistant Cryptography and Quantum Key Distribution.
22	RWP 2.3.2	Will DISA consider the proposed cost of any license under Section 2.3.2 in its evaluation and selection?	No, the proposed cost of any license should be included in section 3.4.5 the Price Evaluation Factor. Any costs associated with licenses shall be included within the "Material/Equipment" ROM line within table # 2 and the ROM narrative shall discuss the approach used to estimate the license price.
23		Some experts on this subject matter may not be US citizens and/or may not have the ability to obtain a security clearance. To ensure that vendors can bring the best expertise to develop a solution, we recommend that the government allow participation by non us citizens and consider placing citizenship and/or clearance requirements on those personnel that will perform work on the DoD infrastructure or on those that have access to classified information, if any, or any other qualifying requirement, as deemed appropriate by the government. Does the government concur? If no, can the government provide details around required citizenship and/or clearances prior to vendor white paper submission?	Due to the sensitivity of information (e.g., ports, protocols, integration points, etc.) that the Government will be required to provide to the selected vendor, the Government will require background investigation for all personnel supporting the prototype effort in accordance with DoD, OPM, and OMB policies. The personnel security requirements could depend upon, the vendor proposed solution, data storage requirements, required information to existing Government data and systems. Therefore the Government will provided additional details regarding the required security clearances in the RFPP. Additional information regarding personnel background investigation is located within the DoD Cloud Computing Requirements Guide and the DoDI 8500.01.

24		To be in a position to offer solutions to the Government in this advanced domain, any organization (to include Traditional Defense Contractors) have likely invested significant monies in R&D and other development to support their proposed capability. In other OTA acquisitions, investment companies have made to date (R&D, IRAD etc.) has been considered acceptable as part of the 1/3 cost share required under 10 U.S.C Section 2371b(d)(1). Will the Government recognize and accept investment already made in the form of R&D or IRAD (by TDCs or others) as part of the 1/3 cost share requirement?	Except as provided in subparagraph (B), the amounts counted for the purposes of this subsection as being provided, or to be provided, by a party to a transaction with respect to a prototype project that is entered into under this section other than the Federal Government do not include costs that were incurred before the date on which the transaction becomes effective.
25	RWP 3.4.3	The section on Security evaluation has the following criteria that are relevant for Quantum Key Distribution but not for Quantum Safe Cryptography. Can this be clarified? - Support same key generation rate as the original decoy state BB84 Quantum Key Distribution (QKD), E91 methods/protocols and other cryptography standards; - Allow for Continuous-Variable (CV) QKD encoded onto the amplitude and phase quadratures of a coherent laser, and methodology for measurement; Detect manipulation based attacks such as, but not limited to: a) Basis-Dependent (Control Attacks) – Perform Intercept-Resend on quantum channel and then hide the disturbance by blinding all signals measured in a different basis. b) State-Dependent (Suppression Attacks) – Blind all detector results except for one pre-chosen state that is chosen uniformly at random for each signal. (e.g., the detector dead-time attack). - Describe results from previous security audits or tests that show how the proposed solution successfully prevented an attack?	The Government has removed this requirement. See updates in section 3.4.3.
26		Is the government considering decentralized key management as part of the quantum resistance strategy?	The Government does not have a pre-defined key management approach and will consider a centralized or decentralized management approach for the quantum resistance strategy.

27		Can the government please release an interested vendors list to the public?	The Government does not have a pre-defined interested vendor list. This Request for White Paper is being used to help the Government identify interested vendors who can meet the proposed requirements.
28	RWP 2.3	In Lieu of a patent, would the government like to see the statements signed by all company employees who supported porotype development? Or would a brief statement verifying that all company employees have signed suffice?	The Company Name can be replaced with "Submitter's Full Name" for sections 2.3.1, 2.3.2, and 2.3.3. All employees do not have to sign the statements, only one signature is required from the Company Representative. If the proposed solution does not have a patent that should be indicated within the final submission and the Proposed Data Rights Assertion in section 3.4.6 should be completed.
29		Can the Government clarify the requirement for a world-wide license?	Section 2.3.2 Patent Owner(s) Statement requires the Patent Owner or authorized representative of a proposed standard/algorithm requires consideration of a non-exclusive license for the purpose of implementing the DoD prototype. There is no statement in the RWP about the Government requiring a "free worldwide license", however the Government will require non-exclusive, non-transferable, irrevocable licenses for the purpose of modifying source code, if required based on the proposed solution. Additional license terms and conditions will be discussed during final negotiations with the selected vendor. License terms and conditions must be demonstrably free of any unfair discrimination. The vendor can include additional Proposed Data Rights Assertion in section 3.4.6. See question #18 for additional detail on interested parties. The proposed cost of any license should be included in section 3.4.5 the Price Evaluation Factor. Any costs associated with licenses shall be included within the "Material/Equipment" ROM line within table # 2.
30	RWP 2.3.3	Will the Government requires copies of hardware or devices as part of the evaluation phase?	The Government does not require vendors to provide copies of hardware or devices for evaluation purposes and requests that additional details be included within the final submission. However if the proposed solution is selected the vendor will be required to grant the U.S. Government and any interested party the right to

			reproduce, prepare derivative works based upon, distribute copies of, and display such implementations notwithstanding that the implementations may be copyrighted or copyrightable.
31		Is the requirement for any 541 (Ex: 541690 Other Scientific and Technical Consulting Services) or is the requirement that the prime vendor must have 541519 specifically? Can the Government clarify the NACIS code for this effort?	The Affirmation of Business Status Certification table on page 8 affords Vendors the opportunity to propose an appropriate NAICS code for this OTA.