DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Other Transaction Authority (OTA)

Request for White Papers (RWP)

Project Number	DISA-OTA-22-9-QRC
RWP Title	Quantum Resistant Cryptography Public Key Infrastructure
Issued by	Defense Information Systems Agency (DISA) Other Transaction (OT) Agreements Team www.DISA.mil
*** White Papers Due Date/Time (Suspense)**	**23 September 2022, 9 AM CST**
Submit White Papers To	disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil, vanessa.a.mccollum.civ@mail.mil, craig.j.carlton.civ@mail.mil

Note: Please advise DISA as soon as possible via email to vanessa.a.mccollum.civ@mail.mil, craig.j.carlton.civ@mail.mil and disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil if your organization intends to submit a White Paper to DISA in response to this RWP.

***White papers are due on 16 September at 9 AM CST. White papers must be received by (be in the inbox of) the Agreements Officer (vanessa.a.mccollum.civ@mail.mil) and Agreements Specialist (craig.j.carlton.civ@mail.mil). Any submissions that received by the Agreements Officer/Agreements Specialist after the deadline will be deemed late and may be eliminated from competition and further consideration. It is the sole responsibility of the vendor to ensure that its white paper submission is received in the inbox of the Agreements Officer/Agreements Specialist before the deadline specified above.**

Amendment 0004 is issued to provide responses to vendor questions. See attached Question and Answer document. All other terms and conditions of the RWP remain the same.

Amendment 0003 is issued to provide responses to vendor questions, modify language in the RWP, and extend the due date/response time for the RWP. The revised response time is now September 23, 2022, at 9:00 am CST. All changes to the RWP are highlighted in yellow.

The Defense Information Systems Agency (DISA), Emerging Technology (EM) Directorate through the DISA Procurement Services Directorate (PSD) is seeking White Papers from our industry partners on a proposed solution for quantum resistant cryptography public key infrastructure.

SECTION 1 OVERVIEW/DESCRIPTION

1.1 PURPOSE

Due to growing concerns related to quantum computers, DISA has begun to investigate quantum-resistant or quantum-safe cryptography algorithms. The goal of this research is to evaluate and test cryptographic algorithms that would secure DoD Information Technology (IT) systems against attacks from both quantum and classical computers. This prototype effort will utilize candidate algorithms that have been identified by National Institute of Standards and Technology (NIST) Post-Quantum Cryptography (PQC) and have been selected for standardization, with potential to add additional algorithms within the prototype period of performance, (See https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4).

These algorithms will inform NIST's research on the PQC project as well as allow the DoD to test how to best integrate these algorithms throughout the DoD enterprise.

This request for White Paper (RWP) is being issued to conduct research, development, and testing activities associated with Quantum Resistant Cryptography or Post Quantum Cryptography algorithms.

1.2 STATEMENT OF NEED

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional or classical computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and within the DoDIN.

The security of many commonly used public-key cryptosystems would be at risk. In particular, they would include key-establishment schemes and digital signatures that are based on factoring, discrete logarithms, and elliptic curve cryptography. In contract, symmetric cryptographic primitives, such as block ciphers and hash functions, would not be as drastically impacted. Therefore, DISA is initially focused on securing key-establishment schemes and digital signatures based on NIST candidate algorithms that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks.

The question of when a large-scale quantum computer will be built is a complicated one. While in the past it was less clear that large quantum computers are a physical possibility, many scientists now believe it to be merely a significant engineering challenge. Some engineers even predict that within the next twenty or so years sufficiently large quantum computers will be built to break essentially all public key schemes currently in use. Historically, it has taken almost two decades to deploy our modern public key cryptography infrastructure. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, DoD must begin now to prepare its information security systems to be able to resist attacks from large-scale quantum computers.

Implementing the QRC PKI solution using opensource implementations (such as libOQS, a C programming language) is acceptable, however the Government will expect any alternative solution to be based on mature capabilities that do not require a long and expensive development effort. The contractor must provide a compelling rationale for providing a QRC PKI solution implementation using alternatives to the libOQS libraries.

SECTION 2 GENERAL SUBMISSION REQUIREMENTS

2.1 FORMATTING

Vendors are solely responsible for all expenses associated with responding to this RWP. White Papers shall follow the format described below. Evaluation and selection of the White Papers will be completed based on criteria in Sections 3 and 4. Responding to this RWP does not obligate the Government for costs associated with responding to this notice. The Government reserves the right to cancel this requirement if the Government deems no White Papers satisfy the criteria contained in Section 3.4 and/or no funding becomes available.

Subject to the availability of funds, the DISA/Defense Information Technology Contracting Organization (DITCO) at Scott AFB, IL intends to competitively issue this effort as an OTA Agreement in accordance with 10 U.S.C.4022. If an OTA is awarded from this subject request, the Agreement is not considered a procurement contract and therefore not subject to the Federal Acquisition Regulation (FAR).

The following **White Paper** formatting requirements apply:

- Times New Roman 10 (or larger) single-spaced, single-sided, 21.6 x 27.9 cm (8.5 by 11 inches);
- Smaller type may be used in figures and tables, but must be clearly legible;
- Margins on all sides (top, bottom, left, and right) should be at least 2.5 cm (1 inch);
- *Italic Red* text with brackets borders (e.g. *[company name]*) indicated areas for entry of information by the vendor. Delete all italicized text, contained within brackets before submittal of the White Paper;
- Page limitations shall not be circumvented by including inserted text boxes/pop-ups or internet links to additional information. Such inclusions are not acceptable and will not be considered as part of the response to Request for White Papers; and
- **DO NOT SUBMIT ANY CLASSIFIED INFORMATION.**
- Page limit for the White Paper submission is fifteen (15) pages. Table below provides guidance on the page limitation and white paper organization:

WP Section Title	PAGE LIMIT
Cover Sheet	N/A
Intellectual Property Statement/Agreements/Disclosures (RWP Section 2.3)	N/A
Affirmation of Business Status Certification (RWP Section 2.4)	N/A 2 pages for prime vendor and 2 pages for each subvendor
Conflict of Interest Statement (RWP Section 2.5)	N/A
Technical and Security (RWP Sections 3.4.1 and 3.4.2)	15 Pages

Business Viability (RWP Section 3.4.3)	N/A
Schedule (RWP Section 3.4.4)	N/A
Price (RWP Section 3.4.5) Narrative (Separate Document) Pricing Spreadsheet	See below 2 N/A
- Rough Order of Magnitude (ROM) Template	N/A
- ROM Narrative	N/A
Data Rights Assertion (RWP Section 3.4.6)	N/A
Participants (RWP Section 3.4.7)	N/A
Implementation of Section 889(a)(1)(B) (RWP Section 7)	N/A
Table of Content	N/A
Acronym list	N/A

A White Paper **Cover Sheet** is required for all submission and must include the following:

- OTA Project Number;
- Project Title;
- Company Title/Name of Proposed Cryptosystem;
- Date of Submittal;
- Primary point of contact (POC), including name, address, phone, and e-mail contact information;
- Total ROM cost for the 16-month period of performance; and

- Disclosure of Information Statement (section 5.2).

2.2 MINIMUM ACCEPTABILITY

The Government will evaluate RWP submissions that are deemed as "complete". To be considered "complete" submissions must contain at a minimum the following:

- Cover Sheet (section 2.1);
- Signed Intellectual Property Statements / Agreements / Disclosures (section 2.3) from the Prime Vendor and all Subvendors. *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 compliance with the outlined requirements;
- Signed Affirmation of Business Statement (section 2.4) from the Prime Vendor and all Subvendors;
- Conflict of Interest (COI) (section 2.5) from the Prime Vendor and all Subvendors;
- Address all the Evaluation Criteria Factors (sub-sections 3.4.1– 3.4.7).
- Implementation of Section 889(A)(1)(B) of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 (section 7)

If the vendor fails to include/address the minimum acceptability requirements (as defined above and throughout the RWP) the White Paper submission may be deemed non-compliant and inadequate for further evaluation. Additionally, if a misrepresentation is found within a White Paper submission (Affirmation of Business Status Certification, Conflict of Interest, and/or Participants) the White Paper may be deemed non-compliant and may not be further evaluated.

2.3 INTELLECTUAL PROPERTY STATEMENT/AGREEMENTS/DISCLOSURES

2.3.1 SUBMITTER STATEMENT

Each participant (prime vendor and each subvendor) shall complete the submitter statement below. The statement shall be included as an attachment to the White Paper and will not count toward the page limit.

I, *[insert submitter's full name]*, of *[insert full postal address]*, do hereby declare that the cryptosystem prototype, that I have submitted, known as *[insert name of cryptosystem[1]]*, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

[1] A cryptosystem is a suite of cryptographic algorithms needed to implement a particular security service, most commonly for achieving confidentiality (encryption). Typically, a cryptosystem consists of three algorithms: one for key generation, one for encryption, and one for decryption.

I further declare that *[check one]*:

☐ I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem prototype that I have submitted, known as *[insert name of cryptosystem]*;

OR *[check one or both of the following]*:

☐ to the best of my knowledge, the practice of the cryptosystem, standards, or algorithms that I have submitted, known as *[insert name of cryptosystem]*, may be covered by the following U.S. and/or foreign patents: *[describe and enumerate or state "none" if applicable]*;

☐ I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, standards, or algorithms *[describe and enumerate or state "none" if applicable]*.

I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications, which may cover my cryptosystem, standards, or algorithms.

I do hereby agree to provide the statements required by Section 2.3.2 and 2.3.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, standards, or algorithms and the right to use such for the purposes of the evaluation process.

Signature (electronic signature is acceptable)	X _____
Name	*[Insert Name of Representative]*
Title	*[Insert Title of Representative]*
Date	*[Insert Date of Signature]*

2.3.2 PATENT OWNER(S) STATEMENT

Each participant (prime vendor and each of the subvendors) shall complete the Patent Owner(s) statement below. The statement shall be included as an attachment to the White Paper and will not count toward the page limit.

If there are any patents (or patent applications) identified by the submitter, including those held by the submitter, the following statement must be signed by each owner, or each owner's authorized representative, of each patent and patent application identified. *Note: For the purpose of the Prototype OTA RWP, an interested party is any party that needs to have access to the solution as part of its performance.

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]*:

☐ without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination,

OR

☐ under reasonable terms and conditions (identified in section 3.4.6 –Proposed Data Rights Assertion) that are demonstrably free of any unfair discrimination.

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of evaluating the proposed cryptosystem prototype. Any future follow-on Production Contract could/will require re-negotiated terms and conditions.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are intended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer documents.

I further do hereby grant to the U.S. Government, during the evaluation process, and during the lifetime of the standard, a nonexclusive, non-transferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the prototype efforts.

Signature (electronic signature is acceptable)	X_____
Name	*[Insert Name of Representative]*
Title	*[Insert Title of Representative]*
Date	*[Insert Date of Signature]*

2.3.3 REFERENCE OWNER(S) STATEMENT

Each participant (prime vendor and each subvendor) shall complete the Reference Statement below. The statement shall be included as an attachment to the White Paper and will not count toward the page limit.

I, *[insert full name]*, *[insert full postal address]*, am the owner or authorized representative of the owner *[insert full name, if different than the signer]* of the submitted reference cryptosystem's specifications and hereby 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 for the purposes of the quantum-resistant evaluation process, and if the corresponding cryptosystem is selected for DoD quantum-safe algorithm and cryptographic standard prototype, notwithstanding that the implementations may be copyrighted or copyrightable.

Signature (electronic signature is acceptable)	✕ _____
Name	*[Insert Name of Representative]*
Title	*[Insert Title of Representative]*
Date	*[Insert Date of Signature]*

2.4 AFFIRMATION OF BUSINESS STATUS CERTIFICATION

Each participant (prime vendor and each subvendor) shall complete the certification below. The certification shall be included as an attachment to the White Paper and will not count toward the page limit. Please note that some sections in the certification may be left blank due to the type of business completing this form (e.g., non-traditional contractor).

Please note that to be eligible to submit a response to the Request for White Paper (RWP), vendors must meet the requirements outlined in 10 U.S.C Section 4022(d)(1). Vendors shall explain in their White Paper submission how they will meet these statutory requirements. The page limitation for this submission shall be two (2) pages for the prime vendor and two (2) pages for each subvendor. Failure to provide the required explanation may result in your White Paper not being considered for this OTA effort.

Participant Name	*[Insert Participant Name]*
Proposed North American Industry Classification System (NAICS) Code	*[Insert NAICS Code]*

Industry Size Standard	*[Check one of the following boxes]* ☐ **Small** ☐ **Large** ☐ **Federally Funded Research & Development Center**
Data Universal Numbering Systems (DUNS) Number	*[Insert DUNS Number]*
Commercial & Government Entity (CAGE) Code	*[Insert CAGE Code]*
Active System for Award Management (SAM) Registration	*[Check one of the following boxes and insert date]* ☐ **Yes** ☐ **No** **Expiration Date:**
Address 1	*[Insert Address Number and Street]*
Address 2	*[Insert suite, office, etc. Number]*
City/State/Zip Code	*[Insert City, State, Zip Code]*
Point of Contact (POC) Name/Title	*[Insert POC Name and Title]*
POC Phone/Email	*[Insert POC Phone and Email]*

[Check one of the following boxes:]

☐ **Nontraditional Defense Contractor (NDC):** A NDC is an entity that is not currently performing and has not performed, for at least the one-year period preceding the issuance of this Request for White Papers by the DoD, any contract or subcontract for the DoD that is subject to full coverage under the cost accounting standards prescribed pursuant to section 1502 of title 41 of the U.S. Code and the regulations implementing such section. All small businesses are considered NDCs. A small business is a business concern as defined under section 3 of the Small Business Act (15 U.S.C. 632). To be considered a small business for the purposes of this RWP, a concern must qualify as a small business under the size standard for the North American Industry Classification System (NAICS) code, as described at 13 C.F.R. 121.201 and the proposed NAICS code above.

☐ **Traditional Defense Contractor:** A traditional defense contractor is an entity that does not meet the definition of a NDC. Any traditional defense contractors must comply with 10 U.S.C Section 2371b(d)(1)(C) to be eligible to submit an RWP.

This is to certify that the above is accurate, complete, and current as of *[MM/DD/YYYY]* for DISA-OTA-19-R-Quantum.

Signature (electronic signature is acceptable)	X _____
Name	*[Insert Name of Representative]*
Title	*[Insert Title of Representative]*
Date	*[Insert Date of Signature]*

2.5 CONFLICT OF INTEREST (COI)

Each vendor (prime vendor and each subvendor) shall specifically state in the white paper, whether there are any potential, actual or perceived conflicts of interest (COI) involving this OTA. If a vendor identifies a potential/actual or a perception of COI, then the vendor shall submit a statement with the white paper explaining how the COI will be mitigated and/or avoided. If the Government determines a COI (potential or actual) or a perception of COI exists and was not identified by the vendor, the white paper may be found non-compliant AND inadequate for further evaluation.

SECTION 3 EVALUATION APPROACH

The Government will employ a three-phased evaluation approach for the award of the Quantum Resistant Cryptography prototype OTA. An award may be made to the responsible vendor whose offer, conforming to the requirements outlined in the RWP, is determined to be the best overall value to the Government, price, and other factors considered. The evaluation criteria are outlined in sub section 3.4.1 – 3.4.7.

Throughout the evaluation, the Government reserves the right, but is not obligated, to ask questions about individual vendor solutions. However, any response to the RWP that does not fully address all of requirements may be eliminated from further consideration. This RWP constitutes Phase I of the evaluation, described below.

Please note that elements of the evaluation approach phases listed below will be dependent upon the Government's acquisition and procurement strategy for a particular OTA prototype. However, industry can generally expect that the phases below will be representative of the evaluation approach.

3.1 PHASE I – WHITE PAPER EVALUATION

The Government will conduct an evaluation of all eligible White Paper(s) submitted in response to this RWP. The White Papers will be evaluated to identify viable solutions. Final selection(s) recommendation(s) will be made by the program management technical lead to the Agreements Officer (AO). After the evaluation of White Paper(s), the Government may select a solution and proceed to the next phase. Any vendor whose solution is not selected will not be provided a debriefing as OTAs are not subject the FAR but, rather, will be provided a letter containing a brief explanation for non-selection.

3.2 PHASE II – ORAL PRESENTATIONS

The Government will invite selected vendors to provide oral presentations, which can be conducted in person or via videoconference. During the presentation, a vendor should be prepared to discuss, in detail, its solution, which includes but is not limited to:

(1) discussion of which NIST quantum safe encryption algorithms you have selected to use and why,
(2) demonstration of all QRC PKI IP or web-based protocols you have already implemented and have working,
(3) demonstration of any QRC PKI Certificate Authority implemented,
(4) demonstration of all QRC PKI-Enabled applications or services you have implemented,
(5) how you would provide a Test Harness for QRC PKI performance testing,
(6) what is your approach for detecting the type of PKI (classical vs QRC-Enabled) on network systems and devices, and
(7) what you perceive to be the risk areas for your approach and how would you mitigate them.
(8) respond appropriately to risks or concerns identified during white paper evaluation.

After the presentation, the Government will conduct evaluations and determine whether a vendor will proceed to the next phase. Any vendor whose solution is not selected will be provided a letter with brief explanation for non-selection.

3.3 PHASE III – REQUEST FOR PROJECT PROPOSAL

The Government will issue a Request for Project Proposal (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 to engage in negotiations. The Government will provide an initial model OT Agreement to the selected vendor, which will be the Governments opening position for negotiations. Using a collaborative process, the Government and the selected vendor will develop a detailed Project Work Statement (PWS); negotiate Terms and Conditions (T&Cs); agree on milestones, performance standards,

deliverables, and negotiate final price. Once complete and all parties agree, the AO will award a prototype OTA to the selected vendor. If the Government is unable to reach an agreement with the initial selectee, the Government may re-evaluate White Paper Responses and make other selections.

3.4 EVALUATION CRITERIA

The overall evaluation will be based on the integrated assessment of the criteria outlined in sub-sections 3.4.1 – 3.4.7.

Vendors are required to meet all the evaluation requirements, objectives, and representations. Failure to respond to any of the follow evaluation factors listed below (sub-sections 3.4.1 – 3.4.7) may result in elimination from the competition. In addition, the Government has included several templates (e.g., tables, etc.) within several of the evaluation factors outlined below, that identify the minimum level of information that must be included with the final submission. If a vendor fails to include the Government provided templates (identified as required), then such failure may result in the vendor's White Paper submission being deemed non-compliant and inadequate for further evaluation. Vendor submissions shall thoroughly discuss the technical and security requirements outlined in Sections 3.4.1 and 3.4.2. Vendors will be required to demonstrate their solutions if selected to move to Phase II, Oral Presentations.

3.4.1 TECHNICAL

Task 1. Provide a QRC-Enabled Certificate Authority.

The vendor shall provide a prototype of a QRC-Enabled Certificate Authority.

1.1 The vendor shall provide a QRC-Enabled Certificate Authority that implements all eight of the NIST candidate QRC algorithms:

- a. CRYSTALS-Kyber
- b. SIKE
- c. CRYSTALS-Dilithium
- d. FALCONS
- e. SHINCS+
- f. BIKE
- g. Classic McEliece
- h. HQC

1.2 The vendor shall provide a QRC-Enabled Certificate Authority that is capable of generating QRC-Enabled X.509 compliant certificates to support post-quantum authentication and digital signatures.

1.3 The vendor shall provide a QRC-Enabled Certificate Authority prototype that implements services/APIs for doing the following:

i. Viewing Certificates
j. Creating Certificates
k. Deleting Certificates
l. Requesting Certificates
m. Delivering Certificates

1.4 The vendor shall provide a QRC-Enabled Certificate Authority prototype that is able to be deployed and operated in a Government test facility that will not have reach back to the Internet.

1.5 The vendor shall provide a QRC-Enabled Certificate Authority prototype that is capable of being extended to issue hybrid certificates that consist of QRC-enabled certificates and PKI-based certificates (see Task 6).

Task 2. Implement QRC-Enabled IP and Web Protocols.

The vendor shall modify/extend existing IP and Web protocols to support the NIST candidate QRC algorithms.

2.1 At a minimum, the vendor shall provide QRC-enabled versions of the following IP and Web protocols:

a. Transport Layer Security (TLS) protocol
b. Secure Shell (SSH) protocol
c. Internet Protocol Security (IPSEC) protocol
d. Secure/Multipurpose Internet Mail Extensions (S/MIME) protocol

2.2 Vendors are encouraged to utilize the open source implementations of these protocols available at https://github.com/open-quantum-safe/liboqs, however, alternative implementations are acceptable, provided they provide equal or greater functionality.

Task 3. Provide a QRC-Enabled PKI Ecosystem.

The vendor shall provide a complete QRC-Enabled PKI Ecosystem prototype that allows the Government to exercise all the functions one would find in a classical (i.e., non-QRC-Enabled) PKI Ecosystem. The QRC-Enabled PKI Ecosystem shall meet the following:

3.1 Using the QRC-Enabled Certificate Authority (from Task 1) and the QRC-Enabled protocols (from Task 2), the vendor shall provide an integrated QRC-enabled PKI Ecosystem prototype. The prototype shall enable the demonstration and assessment of all aspects of classical PKI transactions, but shall do so using QRC-enabled Certificate services and protocols.

3.2 Within the QRC-Enabled PKI Ecosystem, the vendor shall provide and demonstrate the following set of QRC-enabled services:

a. QRC-enabled Web Server.

QRC-enabled Web Browser.

QRC-enabled Email.

QRC-enabled Digital Signatures.

QRC-enabled IPSec VPN Tunnels from site to end-point (PC and mobile devices).

QRC-enabled Web Application Proxy:

3.3 The vendor shall ensure that all elements of the QRC-Enabled PKI Ecosystem prototype can operate in an isolated Government network without the need for Internet reach back.

3.4 The vendor shall provide instrumentation of the QRC-Enabled PKI Ecosystem components to support the assessment and performance testing activities that will be conducted as part of Task 4.

Task 4. Provide a Test Harness for QRC-Enabled PKI Ecosystem Performance Assessment.

The vendor shall provide a Test Harness that is constructed to exercise the various components of the QRC-Enabled PKI Ecosystem (from Tasks 1, 2 and 3) and to enable performance assessment of the QRC-enabled encryption algorithms, QRC-enabled protocols, and QRC-Enabled services.

4.1 The vendor shall provide a QRC Test Harness that exercises the following elements of the PKI Ecosystem:

a. The QRC-Enabled Certificate Authority (from Task 1)
b. The QRC-Enabled Protocols (from Task 2)
c. The QRC-Enabled Services (from Task 3)

d. Interactions of components across the entire QRC-Enabled PKI Ecosystem

4.2 The vendor shall provide a QRC Test Harness that can measure performance impacts of the QRC-Enabled PKI Ecosystem (for desktop, laptops and mobile devices) across the following areas:

a. Compute performance impacts
b. Storage performance impacts
c. Network performance impacts
d. Other performance impacts as identified by the vendor

4.3 The vendor shall provide a QRC Test Harness that allows for performance testing under a range of loading and environmental conditions.

4.4 The vendor shall provide a QRC Test Harness that is able to collect performance data on the following performance differences between the QRC-Enabled PKI Ecosystem and a classic-PKI Ecosystem

a. Differences in transaction speed.
b. Differences in transaction latency.
c. Differences in transaction overhead
d. Other differences as recommended by the vendor

4.5 The vendor shall provide a QRC Test Harness that can be set up to run large batch jobs of performance evaluations that can run to completion without the need for user oversight.

4.6 The vendor shall ensure that all elements of the QRC Test Harness can operate in an isolated Government network without the need for Internet reach back.

4.7 The vendor shall provide a QRC Test Harness that supports the ability to swap in new or updated NIST QRC algorithms as new candidates become available.

4.8 The vendor shall assess the size, storage and access time impacts of NIST QRC algorithms on existing smart cards (e.g., CAC) and certificates for mobile devices.

Task 5. Provide a Crypto Discovery Service.

The vendor shall provide a crypto discovery service that captures, categorizes and presents the various versions of encryption configured and deployed on systems and networks.

5.1 The vendor shall provide a crypto discovery service that identifies and returns information to the requestor on what types and versions of encryption algorithms and protocols are configured and running on DoD networks, systems, endpoints (desktop, laptops and mobile devices) for both:

a. QRC enabled encryption algorithms and protocols
b. classical encryption algorithms and protocols

5.2 The vendor shall provide a Crypto Discovery Service that includes a web-based user interface to allow individuals to interact with the Crypto Discovery Service.

Task 6. Extend the QRC-Enabled PKI Ecosystem to Support Hybrid Operations.

For the purposes of this efforts, we define hybrid operations as a PKI ecosystem that simultaneously supports both QRC-Enabled PKI and classic PKI (non-QRC-Enabled).

The vendor shall extend their QRC-Enabled PKI Ecosystem (developed in Tasks 1, 2, and 3) to support hybrid operations.

6.1 The vendor shall demonstrate user authentication using classical and QRC certificates.

6.2 The vendor shall demonstrate digital signatures using classical and QRC certificates.

6.3 The vendor shall demonstrate hybrid operations using TLS, SSL and IPSec.

3.4.2 SECURITY

The Government will evaluate the vendor's security approach based on the criteria listed below:

Security Requirement 1. Citizenship.

All personnel performing on or supporting work on this OTA in any capacity shall be U.S. citizens.

Security Requirement 2. Personnel Security Clearances.

Most of the work on this OTA can be performed at the unclassified level, however, some of the Technical Requirements will require personnel cleared to the SECRET level. Vendor personnel shall require SECRET clearances to:

c. Get physical access to Government facilities
d. Perform software installation and configuration on Government computer systems.
e. Obtain access to Government threat analyses and vulnerability studies that may shape the implementation of the QRC-Enabled PKI Ecosystem prototype.

Security Requirement 3. Facility Clearances.

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.

Security Requirement 4. Visit Requests.

Visit requests shall be processed and verified through the Joint Personnel Adjudication System (JPAS) to SMO DKABAA10. JPAS visits for contracts/orders are identified as "Other" or "TAD/TDY" and will include the Contract/Order Number and ADP/IT-Access level of the contract/order in the Additional Information Section. Vendors that do not have access to JPAS may submit visit authorizations by e-mail in a password protected .pdf to the Contracting Officer Representative (COR) or Alternate COR. If JPAS is not available, the VAL must contain the following information on company letterhead:

f. Company name, address, telephone number, facility security clearance
g. CAGE CODE
h. Contract/Order Number
i. Name, SSN, date and place of birth, and citizenship of the employee intending to visit
j. Certification of personnel security clearance and any special access authorizations required for the visit (type of investigation & date, adjudication date & agency, and IT access level)
k. Name of AOR/Alt AOR
l. Dates or period the VAL is to be valid

Security Requirement 5. Other Security Requirements.

The vendor shall comply with the following DISA security requirements in the course of conducting the work under this OTA contract.

5.1 Vendor personnel shall comply with all local security requirements including entry and exit control for personnel and property at the government facility.

5.2 Vendor employees shall be required to comply with all Government security regulations and requirements. Initial and periodic safety and security training and briefings will be provided by Government security personnel. Failure to comply with Government security regulations and requirements shall require the company to provide the Government with a written remediation/corrective action plan; furthermore, failure to comply with such requirements can be cause for removal and the contractor will not be able to provide service on this contract/order.

5.3 Vendor employees with an incident report in JPAS who have had their access to classified suspended will not be permitted to fill positions requiring access to classified information on a DISA contract/order.

5.4 The Vendor shall not divulge any information, classified or unclassified, about DoD files, data processing activities or functions, user identifications, passwords, or any other knowledge that may be gained, to anyone who is not authorized to have access to such information. The Contractor shall observe and comply with the security provisions in effect at the DoD facility. Identification shall be worn and displayed as required.

5.5 DISA retains the right to request removal of vendor personnel regardless of prior clearance or adjudication status, whose actions, while assigned to this contract, clearly conflict with the interest of the Government.

5.6 Vendor personnel will generate or handle documents that contain For Official Use Only information at the Contractor and Government facility. Contractor personnel will have access to, generate, and handle classified material up to the SECRET level only at the location(s) listed in the place of performance section of this document. All contractor deliverables shall be marked in accordance with DoDM 5200.01, Vol. 3, Vol. 4, Information Security, DoDM 5400.07, Freedom of Information Act Program, unless otherwise directed by the Government. The contractor shall comply with the provisions of the DoD Industrial Security Manual for handling classified material and producing deliverables. The contractor shall comply with DISA Instruction 630-230-19, Cybersecurity.

3.4.3 BUSINESS VIABILITY

Business viability shall be included as an attachment to the White Paper and will not count toward the page limit. Please address whether the company has the technical capability and resources to effectively accomplish the work. The White Paper should also address the following:

- Describe your company. How old is it?
- Where is it located (e.g., multiple locations, sales/R&D in U.S. and other countries)?
- How many employees does your company employ?
- Describe the management team – who are they? What are their backgrounds and history?
- What is your annual revenue (sales and costs)?

3.4.4 SCHEDULE

The Government will evaluate the vendors proposed schedule/timeline/sprints to include milestones, activities, and deliverables to research, evaluate, test, and deliver a prototype. The multifaceted concept exploration and design approach must demonstrate the vendor's ability to provide the Government with a complete QRC PKI ecosystem solution and a comprehensive QRC Test Harness for assessing the QRC PKI ecosystem performance.

Table 1 – Schedule

Phase	Milestone	Deliverable	Estimated Delivery (Weeks/Months after Award)
Phase 1	Setup CA with NIST algorithms and issue Post-Quantum certificates	• CA Design Documents • CA Code Base* • CA Installation Guide • CA Users Guide	4 months
Phase 1	Implement QRC-enabled TLS, SSH protocols	• Protocol API Specs • Protocol Code Base*	4 months
Phase 1	Demonstrate PQ PKI user authentication	• PQ PKI Demonstration Plan • PQ PKI Systems Flow Matrix (SV-6)	4 months
Phase 2	Implement QRC-enabled IPSec, S/MIME protocols	• Protocol API Specs • Protocol Code Base*	8 months
Phase 2	Demonstrate full PKI Ecosystem (user authentication, web server, web browser, web proxy server, Email, Digital Signatures, and VPN Tunnels)	• Design Documents • Code Base • Installation Guide • User Guide	Initial: 8 months Updates every 3 months 16 months (Final)
Phase 2	Complete QRC Test Harness	• Test Harness Design Docs • Test Harness Code Base* • Installation Guide • User Guide	16 months (Final

Phase	Milestone	Deliverable	Estimated Delivery (Weeks/Months after Award)
Phase 2	Demonstrate Crypto Discovery Tools for Asset Discovery	• Asset Discovery Design Docs • Asset Discovery Code Base* • Installation Guide • Users Guide	16 months (final)
Phase 2	Demonstrate Hybrid Operation of QRC PKI Ecosystem	• Hybrid Design Docs • Hybrid Code Base* • Installation Guide • User Guide	Initial Demo: 12 months Final Demo 16 months
Phase 2	Conduct performance assessment benchmarks of the QRC PKI Ecosystem	• QRC PKI Ecosystem Assessment Plan • Non-QRC PKI Baseline Performance results • QRC PKI performance results. • Final Assessment Report	16 months (Final) Initial Report: 8 Months (Updates every 2 months)

3.4.5 PRICE

The vendor shall submit pricing data utilizing the Government's supplied Rough Order of Magnitude (ROM) Template (table 3). Failure to include the information described within this section may result in the vendor's entire Price/Cost criteria/factor being deemed non-compliant and inadequate for further evaluation review.

In making a selection, the Government will consider affordability in comparison to the Government estimate to determine whether the proposed solution is in the best interest of the Government. The Government provided ROM Template (i.e., table 3) shall be included as an addendum or appendix to the White Paper and will not count toward the page limit. The vendor is responsible for verifying that the totals within table 3 are correctly calculated.

The vendor ROM narrative shall be a separate document from the White Paper and discuss the approach, methodology, and basis of estimate used to estimate the price of accomplishing all requirements. The Vendor shall assume the Government knows nothing about its capabilities or estimating approach.

At a minimum, the ROM narrative shall also include the following cost categories for the ROM:

- **Prime Vendor Labor:** The ROM Narrative shall include the basis for which the estimate labor was calculated. (i.e., Generic position titles and estimated fully burdened rates and hours for those individuals).
- **Sub-Vendor/Consultant Labor:** Provide a list of sub-vendor/consultant effort required to meet the technical approach as described in the white paper and the estimated cost. Include the basis for which the estimated labor was calculated, (i.e., Generic position titles and estimated fully burdened hourly rates and hours for those individuals).
- **Material/Equipment:** Provide a list of the materials/equipment required to meet the technical approach as described in the White Paper and the estimated cost.
- **ODCs and/or Travel:** Provide a list of the other direct costs required to meet the technical approach as described in the White Paper and the estimated costs with basis of estimate. Identify any expenses incurred by an employee while those individuals are traveling for business purposes. (e.g., estimated costs for lodging, transportation, and meals) and identify the basis for how the travel costs were calculated.

Table 2 – ROM Template

Elements	FY2023	FY2024	Grand Total
Program/Project Management			
Prime Vendor Labor	*[Insert Total Cost for Prime Labor for Fiscal Year 2023]*	*[Insert Total Cost for Prime Labor for Fiscal Year 2024]*	*[Insert Total Cost for Prime Labor for Fiscal Year 2022-2024]*
Sub – Vendor/Consultant Labor	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2023]*	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2024]*	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2022-2024]*
Material/Equipment	*[Insert Total Cost for Material/Equipment for Fiscal Year 2023]*	*[Insert Total Cost for Material/Equipment for Fiscal Year 2024]*	*[Insert Total Cost for Material/Equipment for Fiscal Year 2022-2024]*
Other Direct Costs (ODCs)and/or Travel	*[Insert Total Cost for ODCs for Fiscal Year 2023]*	*[Insert Total Cost for ODCs for Fiscal Year 2024]*	*[Insert Total Cost for ODCs for Fiscal Year 2022-2024]*
SUBTOTAL	*[Insert Total Cost for Program/Project Management for Fiscal Year 2023]*	*[Insert Total Cost for Program/Project Management for Fiscal Year 2024]*	*[Insert Total Cost for Program/Project Management for Fiscal Year 2022-2024]*
Concept Exploration			
Prime Vendor Labor	*[Insert Total Cost for Prime Labor for Fiscal Year 2023]*	*[Insert Total Cost for Prime Labor for Fiscal Year 2024]*	*[Insert Total Cost for Prime Labor for Fiscal Year 2022-2024]*
Sub – Vendor/Consultant Labor	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2023]*	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2024]*	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2022-2024]*

Material/Equipment	*[Insert Total Cost for Material/Equipment for Fiscal Year 2023]*	*[Insert Total Cost for Material/Equipment for Fiscal Year 2024]*	*[Insert Total Cost for Material/Equipment for Fiscal Year 2022-2024]*
Other Direct Costs (ODCs)and/or Travel	*[Insert Total Cost for ODCs for Fiscal Year 2023]*	*[Insert Total Cost for ODCs for Fiscal Year 2024]*	*[Insert Total Cost for ODCs for Fiscal Year 2022-2024]*
SUBTOTAL	*[Insert Total Cost for Concept Exploration for Fiscal Year 2023]*	*[Insert Total Cost for Concept Exploration for Fiscal Year 2024]*	*[Insert Total Cost for Concept Exploration for Fiscal Year 2022-2024]*
Design Prototype			
Prime Vendor Labor	*[Insert Total Cost for Prime Labor for Fiscal Year 2023]*	*[Insert Total Cost for Prime Labor for Fiscal Year 2024]*	*[Insert Total Cost for Prime Labor for Fiscal Year 2022-2024]*
Sub – Vendor/Consultant Labor	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2023]*	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2024]*	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2022-2024]*
Material/Equipment	*[Insert Total Cost for Material/Equipment for Fiscal Year 2023]*	*[Insert Total Cost for Material/Equipment for Fiscal Year 2024]*	*[Insert Total Cost for Material/Equipment for Fiscal Year 2022-2024]*
Other Direct Costs (ODCs)and/or Travel	*[Insert Total Cost for ODCs for Fiscal Year 2023]*	*[Insert Total Cost for ODCs for Fiscal Year 2024]*	*[Insert Total Cost for ODCs for Fiscal Year 202-2024]*
SUBTOTAL	*[Insert Total Cost for Design Prototype for Fiscal Year 2023]*	*[Insert Total Cost for Design Prototype for Fiscal Year 2024]*	*[Insert Total Cost for Design Prototype for Fiscal Year 2019-2024]*
Test and Evaluation (T&E)			
Prime Vendor Labor	*[Insert Total Cost for Prime Labor for Fiscal Year 2023]*	*[Insert Total Cost for Prime Labor for Fiscal Year 2024]*	*[Insert Total Cost for Prime Labor for Fiscal Year 2022-2024]*

Sub – Vendor/Consultant Labor	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2023]*	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2024]*	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2022-2024]*
Material/Equipment	*[Insert Total Cost for Material/Equipment for Fiscal Year 2023]*	*[Insert Total Cost for Material/Equipment for Fiscal Year 2024]*	*[Insert Total Cost for Material/Equipment for Fiscal Year 2022-2024]*
Other Direct Costs (ODCs)and/or Travel	*[Insert Total Cost for ODCs for Fiscal Year 2023]*	*[Insert Total Cost for ODCs for Fiscal Year 2024]*	*[Insert Total Cost for ODCs for Fiscal Year 2022-2024]*
SUBTOTAL	*[Insert Total Cost for T&E for Fiscal Year 2023]*	*[Insert Total Cost for T&E for Fiscal Year 2024]*	*[Insert Total Cost for T&E for Fiscal Year 2022-2024]*
TOTAL ROM COSTS			
Prime Vendor Labor	*[Insert Total Cost for Prime Labor for Fiscal Year 2023]*	*[Insert Total Cost for Prime Labor for Fiscal Year 2024]*	*[Insert Total Cost for Prime Labor for Fiscal Year 2022-2024]*
Sub – Vendor/Consultant Labor	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2023]*	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2024]*	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2022-2024]*
Material/Equipment	*[Insert Total Cost for Material/Equipment for Fiscal Year 2023]*	*[Insert Total Cost for Material/Equipment for Fiscal Year 2024]*	*[Insert Total Cost for Material/Equipment for Fiscal Year 2022-2024]*
Other Direct Costs (ODCs)and/or Travel	*[Insert Total Cost for ODCs for Fiscal Year 2023]*	*[Insert Total Cost for ODCs for Fiscal Year 2024]*	*[Insert Total Cost for ODCs for Fiscal Year 2022-2024]*
TOTAL	*[Insert Total Cost of All Elements for Fiscal Year 2023]*	*[Insert Total Cost of All Elements for Fiscal Year 2024]*	*[Insert Total Cost of All Elements for Fiscal Year 2022-2024]*

The Government does not require supporting data to justify the estimated costs (e.g., copies of commercial/market price lists/rates, price history, subcontractor quotes, invoices) with the submission of the White Paper. However, vendors will be required to supply the supporting data upon the Request for Project Proposal, if selected.

3.4.6 DATA RIGHTS ASSERTION

State whether there are any data rights issues that the Government should be cognizant of moving forward. Specifically, please identify any intellectual property, patents and inventions involved in the proposed solution and associated restrictions on the Government's use of that intellectual property, patents and inventions. The following table shall be presented for all assertions.

Table 3 – Data Rights Assertion

Technical Data/Computers Software/ Patent to be Furnished with Restrictions	Basis for Assertion	Asserted Rights Category	Name of Entity Asserting Restrictions
[Identify the technical data/software/patent to be furnished with restriction]	*[Indicate whether development was exclusively or partially at private expense. If development was not at private expense, enter the specific reason for asserting that the Government's right should be restricted]*	*[Insert asserted rights category (e.g., limited rights (data), restricted rights (software), government purpose rights, SBIR data rights or specifically negotiated license)]*	*[Insert asserted rights category (e.g., limited rights (data), restricted rights (software), government purpose rights, SBIR data rights or specifically negotiated license)]*

3.4.7 PARTICIPANTS

List all participants (i.e., other vendors), including description of contributions and significance of each participant.

Table 4 – Participants

Participant	Business Status (Check one)	Participant Contribution and Significance to Overall Project
[Insert separate row(s) for each additional participant. Delete row(s) as applicable if Participant is the only participant.]	☐ *Traditional* ☐ *Non-Traditional*	*[Insert detailed, quantifiable description which addresses the following:* • *What is this Participant's significant contribution?* • *Why is this Participant's contribution significant to the overall project?* • *How is this Participant uniquely qualified to provide this significant contribution?*

		(Note: number of years of experience is not deemed a unique qualification.)]

The facility(ies) where the proposed work is to be performed and the equipment or other Participant property which will be utilized for the prototype include: *[Insert a brief description of facility(ies)/equipment proposed for use on the project]*.

SECTION 4 AWARD

4.1 SELECTION DECISION

It is the Government's intention to negotiate, select, and fund a Prototype Project at the conclusion of the three-phased evaluation approach, described in Section 3, which best meets the evaluation criteria listed in Sub-Section 3.4. The White Paper selection will be conducted in accordance with Government procedures and the evaluation criteria in Sub-Section 3.4. The Government will make a determination whether to:

- Select the White Paper(s), or some portion of the White Paper(s); or,
- Reject the White Paper(s) for further consideration.

The White Paper basis of selection decision will be formally communicated to vendors in writing. Once the selection of the best solution(s) is made, the Government team may proceed to the next phase of the evaluation. At any time during evaluations, the Government may choose to cancel this requirement. In case of cancellation, the Government will not be responsible for any expenses associated with responding to RWP.

4.2 FOLLOW ON PRODUCTION

The Government intends to award one (1) prototype OTA. Prior to awarding a prototype OTA, the Government will ensure that it is in compliance with 10 USC §4022(d)(1). The Government will obtain approval from the appropriate approval authority, based on the dollar threshold projected for the prototype OTA. This will be done prior to entering into the prototype OT with a selected vendor.

Provided that the prototype OTA is successfully completed, the Government may award a follow-on production FAR-based contract or OTA to the participant in the transaction for the prototype project, without further competition. If it is determined that transition activities are in the best interest of the Government, then the Government reserves the right to bilaterally modify the Agreement by adding such activities. Prior to award of the production contract or transaction, the Government will ensure that it is in compliance with 10 USC 4022(f). In addition, the Government will again obtain approval from the appropriate approval authority, based on the dollar threshold projected for the production FAR-based contract or production OTA.

SECTION 5 ADDITIONAL INFORMATION

5.1 DOCUMENTATION CLASSIFICATION

Vendors shall not submit any documentation that is classified as "Confidential," "Secret," or "Top Secret" throughout the evaluation process. This includes, but is not limited to submission of White Papers, Project Proposals, Project Work Statements, etc.

5.2 DISCLOSURE OF INFORMATION

White Papers, Project Proposals, PWS, etc. containing data that is not to be disclosed to the public for any purpose or used by the Government except for evaluation purposes shall include the following sentences on the cover page:

"This white paper includes data that shall not be disclosed outside the Government, except to non-Government personnel for evaluation purposes, and shall not be duplicated, used, or disclosed -- in whole or in part -- for any purpose other than to evaluate this submission. If, however, an agreement is issued to this Company as a result of -- or in connection with – the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent agreed upon by both parties in the resulting agreement. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained in sheets *[insert numbers or other identification of sheets]."*

Non-Government personnel ☐X will, ☐ will not be used in the evaluation of the White Papers. The non-Government advisor may have access to all aspects of the offeror's White Paper. By submitting a White Paper, your company agrees with the use of a non-Government advisor employed with the following company(ies):

Company(ies): ManTech/Tapestry – Robert Beaton, Michael Hebert

5.2.1 DATA SHEET MARKINGS

Marking requirements specify that data be "conspicuously and legibly" marked with a protective legend that identifies the OTA number, contractor's name and address, and the submittal date, along with the warning "*Use or disclosure of data contained on this sheet is subject to restriction"* on the title page of any restricted data sheets.

5.3 ANALYTICAL AND LABORATORY STUDIES

It is generally desired that active research and development (R&D) is underway for concepts submitted under this effort. Active R&D includes analytical studies and laboratory studies to physically validate the analytical predictions of separate elements of the technology, as well as software engineering and development. The Government is requesting information on any current or ongoing analytical or laboratory studies related to quantum-safe algorithms and cryptographic solutions. Any information related to ongoing efforts shall be included as an attachment to the White Paper and will not count toward the page limit.

5.4 RECORDS, FILES, AND DOCUMENTATION

All physical records, files, documents, and work papers, provided and/or generated by the Government and/or generated for the Government in performance of this OTA, maintained by the vendor which are to be transferred or released to the Government, shall become and remain Government property and shall be maintained and disposed of as applicable. Nothing in this section alters the rights of the Government or the vendor with respect to patents, data rights, copyrights, or any other intellectual property or proprietary information as set forth in any other part of this RWP (including all clauses that are or shall be included or incorporated by reference into the prototype OTA). The AO may at any time issue a hold notification in writing to the vendor. At such time, the vendor may not dispose of any Government data or Government-related data described in the hold notification until such time as the vendor is notified in writing by the AO, and shall preserve all such data IAW Agency instructions. The vendor shall provide the AO within ten (10) business days of receipt of any requests from a third party for Government-related data. When the Government is using a vendor's quantum-safe algorithms and cryptographic solutions, the vendor shall provide the Agency with access and the ability to search, retrieve, and produce Government data in a standard commercial format.

5.5 SECURITY CLEARANCES

The vendor is responsible for providing personnel with appropriate security clearances to ensure compliance with Government security regulations. The vendor shall fully cooperate on all security checks and investigations by furnishing requested information to verify the vendor employee's eligibility for any required clearance.

The vendors proposed solution (e.g., data, integration with supporting DoD Infrastructure, architecture) will determine the personnel security clearance requirements for the prototype effort. The Government will provided additional details regarding the required security clearances in the RFPP.

5.6 DATA STORAGE

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. The vendor will be required to maintain all government data that is not physically located on DoD premises within the 50 States, the District of Columbia, and outlying areas of the U.S., unless otherwise authorized by the responsible Government, as described in DoDI 8510.01 and the DoD Cloud Computing Security Requirements Guide.

If the Government data is co-located with the non-Government data, the vendor shall isolate the Government data into an environment where it may be reviewed, scanned, or forensically evaluated in a secure space with access limited to authorized Government personnel identified by the Agreements Officer, and without the vendor's involvement. The vendor shall record all physical access to the cloud storage facilities and all logical access to the Government data. This may include the entrant's name, role, purpose, account identification, entry and exit time. Such records shall be provided to the Agreements Officer or designee in accordance with the agreement or upon request to comply with federal authorities.

5.7 LAW ENFORCEMENT

The vendor shall acknowledge and affirm that United States (U.S.) Federal law enforcement officials do not need a warrant or a subpoena to access Government data on any system or media employed by the vendor or their sub-vendors or other partners, or allies, to deliver or otherwise support the contracted service for the U.S. Government, subject to requirements for access to classified information and release thereof, if applicable. As specified by the Agreements Officer, the vendor shall provide immediate access to all Government data and Government-related data impacting Government data for review, scan, or conduct of a forensic evaluation and physical access to any contractor facility with Government data.

5.8 NOTIFICATION

The vendor shall notify the Government Security Contacts (Disa.meade.bd.mbx.sd-security-managers@mail.mil), and the AO within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any Government data. The vendor shall cooperate with the Government to take all measures to protect Government data from any loss or unauthorized disclosure that might reasonably result from the execution of any such warrant, seizure, subpoena, or similar legal process.

5.9 VENDOR INCURRED EVALUATION COSTS

The costs associated with participating in Phases I through III, to include White Paper(s) preparation and submission, are not considered an allowable charges and should not be included within the ROM or any pricing information.

5.10 EXPORT CONTROLS

Research findings and technology developments arising from the resulting White Paper may constitute a significant enhancement to the national defense and to the economic vitality of the United States. As such, in the conduct of all work related to this effort, the recipient will comply strictly with the International Traffic in Arms Regulation (22 CFR 120-130), the National Industrial Security Program Operating Manual (DoD 5220.22-M) and the Department of Commerce Export Regulation (15 CFR 730-774).

SECTION 6 RESPONSES

Questions should be addressed to disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil, Vanessa McCollum at vanessa.a.mccollum.civ@mail.mil and Craig Carlton at craig.j.carlton.civ@mail.mil . Please provide any questions, in writing, no later than 22 August 2022 9AM Central Standard Time (CST). The Government reserves the right to not answer questions submitted after this time. Any submissions that are received after the close of the solicitation period will receive no further consideration.

The response shall be due no later than 16 September 2022 9AM . The responses shall be emailed to disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil, Vanessa McCollum at vanessa.a.mccollum.civ@mail.mil and Craig Carlton at craig.j.carlton.civ@mail.mil . **White papers must be received by (be in the inbox of) the Agreements Officer (vanessa.a.mccollum.civ@mail.mil) and Agreements Specialist (craig.j.carlton.civ@mail.mil). Any submissions that received by the Agreements Officer/Agreements Specialist after the deadline will be deemed late and may be eliminated from competition and further consideration. It is the sole responsibility of the vendor to ensure that its white paper submission is received in the inbox of the Agreements Officer/Agreements Specialist before the deadline specified above.**

SECTION 7 IMPLEMENTATION OF SECTION 889(A)(1)(B) OF THE JOHN S. MCCAIN NATIONAL DEFENSE AUTHORIZATION ACT (NDAA) FOR FISCAL YEAR 2019

REPRESENTATION REGARDING CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (AUG 2020)

The offeror shall not complete the representation at paragraph (d)(1) of this provision if the offeror has represented that it "does not provide covered telecommunications equipment or services as a part of its offered Products or services to the Government in the performance of any contract, subcontract, or other contractual instrument" in the provision at 52.204-26, covered telecommunications equipment or services—Representation, or in paragraph (v) of the provision at 52.212-3, offeror Representations and Certifications-Commercial Items.

(a) Definitions. As used in this provision—

Backhaul, covered telecommunications equipment or services, critical technology, interconnection arrangements, reasonable inquiry, roaming, and substantial or essential component have the meanings provided in the clause 52.204-25, Prohibition on contracting for Certain Telecommunications and Video Surveillance Services or equipment.

(b) Prohibition.

(1) Section 889(a)(1)(A) of the John S. McCain national defense authorization Act for fiscal year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Nothing in the prohibition shall be construed to—

(i)Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii)Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(2) Section 889(a)(1)(B) of the John S. McCain national defense authorization Act for fiscal year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract or extending or renewing a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or

services as a substantial or essential component of any system, or as critical technology as part of any system. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. Nothing in the prohibition shall be construed to—

(i)Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii)Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) Procedures. The offeror shall review the list of excluded parties in the System for Award Management (SAM) (https://www.sam.gov) for entities excluded from receiving federal awards for "covered telecommunications equipment or services".

(d) Representation. The offeror represents that—

(1)It □ will, □ will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation. The offeror shall provide the additional disclosure information required at paragraph (e)(1) of this section if the offeror responds "will" in paragraph (d)(1) of this section; and

(2)After conducting a reasonable inquiry, for purposes of this representation, the offeror represents that—

It □ does, □ does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services. The offeror shall provide the additional disclosure information required at paragraph (e)(2) of this section if the offeror responds "does" in paragraph (d)(2) of this section.

(e) Disclosures.

(1) Disclosure for the representation in paragraph (d)(1) of this provision. If the offeror has responded "will" in the representation in paragraph (d)(1) of this provision, the offeror shall provide the following information as part of the Offer:

(i)For covered equipment—

(A)The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the original equipment manufacturer (OEM) or a distributor, if known);

(B)A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C)Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(ii)For covered services—

(A)If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B)If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(2) Disclosure for the representation in paragraph (d)(2) of this provision. If the offeror has responded "does" in the representation in paragraph (d)(2) of this provision, the offeror shall provide the following information as part of the Offer:

(i)For covered equipment—

(A)The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known);

(B)A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C)Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(ii)For covered services—

(A)If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model

number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B)If not associated with maintenance, the PSC of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (AUG 2020)

(a) Definitions. As used in this clause—

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered foreign country means The People's Republic of China.

covered telecommunications equipment or services means–

(1) Telecommunications equipment produced by Huawei Technologies company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology company, or Dahua Technology company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an

entity owned or controlled by, or otherwise connected to, the Government of a Covered foreign country.

critical technology means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) Prohibition.

(1) Section 889(a)(1)(A) of the John S. McCain national defense authorization Act for fiscal year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain national defense authorization Act for fiscal year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) Exceptions. This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event the contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the contractor is notified of such by a Subcontractor at any tier or by any other source, the contractor shall report the information in paragraph (d)(2) of this clause to the contracting officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the contractor shall

report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the contractor shall report to the contracting officer for the indefinite delivery contract and the contracting officer(s) for any affected order or, in the case of the Department of Defense, identify both the

indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) Subcontracts. The contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

SECTION 8 PRIVACY ACT NOTIFICATION (APR 1984) *[if applicable]*

The will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of1974, Public Law 93-579, December 31, 1974 (5 U.S.C.552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

SECTION 9 PRIVACY ACT (APR 1984) *[Delete if not applicable]*

(a) The Vendor agrees to-

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system ofrecords on individuals to accomplish an agency function when the agreement specifically identifies-

(i) The systems of records; and

(ii) The design, development, or operation work that the vendor is to perform;

(2) Include the Privacy Act notification contained in Article XX of this agreement inevery solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

(3) Include this article, including this paragraph (3), in all subcontracts awarded underthis agreement which requires the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the agreement is for the operation of a system of records on individuals to accomplish an agency function, the Vendor is considered to be an employee of the agency.

(c)

(1) "Operation of a system of records," as used in this article, means performance of any ofthe activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

(2) "Record," as used in this article, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifyingparticular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

(3) "System of records on individuals," as used in this article, means a group of any records under the control of any agency from which information is retrieved by the name ofthe individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

SECTION 10 PRIVACY (APR 1984)

Agencies shall ensure that agreements for information technology address protection of privacy in accordance with the Privacy Act (5 U.S.C. 552a) and part 24. In addition, each agency shall ensure that agreements for the design, development, or operation of a system ofrecords using commercial information technology services or information technology support services include the following:

(a) Agency rules of conduct that the vendor and the vendor's employees shall be required to follow.

(b) A list of the anticipated threats and hazards that the vendor must guard against.
(c) A description of the safeguards that the vendor must specifically provide.
(d) Requirements for a program of Government inspection during performance of the agreement that will ensure the continued efficacy and efficiency of safeguards and the discovery and countering of new threats and hazards.

SECTION 11 AVAILABILITY OF FUNDS

The Government's obligation under this agreement is contingent upon the availability of appropriated funds from which payment for agreement purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are made available to the Agreements Officer for this contract and until the Vendor receives notice of such availability, to be confirmed in writing by the Agreements Officer.

SECTION 12 LIMITATION OF COSTS

The parties estimate that performance of this contract, exclusive of any fee, will not cost the Government more than the estimated cost specified in the Milestone Payment Plan.

(b) The Vendor shall notify the Agreements Officer in writing whenever it has reason to believe that -

(1) The costs the Vendor expects to incur under this agreement in the next 60 days, when added to all costs previously incurred, will exceed 75 percent of the estimated cost specifiedin the Milestone Payment Plan; or

(2) The total cost for the performance of this agreement, exclusive of any fee, will be eithergreater or substantially less than had been previously estimated.

(c) As part of the notification, the Vendor shall provide the Agreements Officer a revised estimate of the total cost of performing this agreement.
(d) Except as required by other provisions of this agreement, specifically citing and stated tobe an exception to this agreement -

(1) The Government is not obligated to reimburse the Vendor for costs incurred in excess of (i) the estimated cost specified in the Milestone Payment Plan; and

(2) The Vendor is not obligated to continue performance under this agreement (including actions under the Termination article of this agreement) or otherwise incur costs in excess ofthe estimated cost specified in the Milestone Payment Plan, until the Agreements Officer (i) notifies the Vendor in writing that the estimated cost has been increased and (ii) providesa revised estimated total cost of performing this agreement.

(e) No notice, communication, or representation in any form other than that specified in subparagraph (d)(2) above, or from any person other than the Agreements Officer, shall affect this agreement's estimated cost to the Government. In the absence of the specified notice, the Government is not obligated to reimburse the Vendor for any costs in excess of the estimated cost, whether those excess costs were incurred during the course of the agreement or as a result of termination.

(f) If the estimated cost specified in the Milestone Payment Plan is increased, any costs the Vendor incurs before the increase that are in excess of the previously estimated cost shallbe allowable to the same extent as if incurred afterward, unless the Agreements Officer issues a termination or other notice directing that the increase is solely to cover termination or other specified expenses.

(g) Change orders shall not be considered an authorization to exceed the estimated cost tothe Government specified in the Milestone Payment Plan, unless they contain a statementincreasing the estimated cost.

(h) If this agreement is terminated or the estimated cost is not increased, the Governmentand the Vendor shall negotiate an equitable distribution of all property produced or purchased under the agreement, based upon the share of costs incurred by each.

SECTION 13 LIMITATION OF FUNDS

(a) The parties estimate that performance of this agreement will not cost the Government more than

(1) the estimated cost specified in the Schedule or, (2) if this is a cost-sharing agreement, the Government's share of the estimated cost specified in the Schedule. The Contractor agrees to use its best efforts to perform the work specified in the Schedule and all obligations under this agreement within the estimated cost, which, if this is a cost-sharing agreement, includes both the Government's and the Contractor's share of the cost.

(b) The Schedule specifies the amount presently available for payment by the Government and allotted to this agreement, the items covered, the Government's share of the cost if this is a cost-sharing agreement, and the period of performance it is estimated the allotted amount will cover. The parties contemplate that the Government will allot additional funds incrementally to the agreement up to the full estimated cost to the Government specified in the Schedule, exclusive of any fee. The Vendor agrees to perform, or have performed, work on the agreement up to the point at which the total amount paid and payable by the Government under the agreement approximates but does not exceed the total amount actually allotted by the Government to the agreement.

(c) The Vendor shall notify the Agreements Officer in writing whenever it has reason to believe that the costs it expects to incur under this agreement in the next 60 days, when added to all costs previously incurred, will exceed 75 percent of (1) the total amount so far allotted to the agreement by the Government or, (2) if this is a cost-sharing agreement, the amount then allotted to the agreement by the Government plus the Contractor's corresponding share. The notice shall state the estimated amount of additional funds required to continue performance for the period specified in the Schedule.

(d) Sixty days before the end of the period specified in the Schedule, the Vendor shall notify the Agreements Officer in writing of the estimated amount of additional funds, if any, required to continue timely performance under the agreement or for any further period specified in the Schedule or otherwise agreed upon, and when the funds will be required.

(e) If, after notification, additional funds are not allotted by the end of the period specified in the Schedule or another agreed-upon date, upon the Vendor's written request the Agreements Officer will terminate this agreement on that date in accordance with the provisions of Article II.B., Early Termination of Agreement Provision, of this agreement. If the Vendor estimates that the funds available will allow it to continue to discharge its obligations beyond that date, it may specify a later date in its request, and the Agreements Officer may terminate this agreement on that later date.

(f) Except as required by other provisions of this agreement, specifically citing and stated to be an exception to this clause -

(1) The Government is not obligated to reimburse the Vendor for costs incurred in excess of the total amount allotted by the Government to this agreement; and

(2) The Vendor is not obligated to continue performance under this agreement (including actions under the Termination article of this agreement) or otherwise incur costs in excess of (i) the amount then allotted to the agreement by the Government or, (ii) if this is a cost-sharing agreement, the amount then allotted by the Government to the agreement plus the Contractor's corresponding share, until the Agreements Officer notifies the Vendor in writing that the amount allotted by the Government has been increased and specifies an increased amount, which shall then constitute the total amount allotted by the Government to this agreement.

(g) The estimated cost shall be increased to the extent that (1) the amount allotted by the Government or, (2) if this is a cost-sharing agreement, the amount then allotted by the Government to the agreement plus the Vendor's corresponding share, exceeds the estimated cost specified in the Schedule. If this is a cost-sharing agreement, the increase shall be allocated in accordance with the formula specified in the Schedule.

(h) No notice, communication, or representation in any form other than that specified in subparagraph (f)(2) above, or from any person other than the Agreements Officer, shall affect the amount allotted by the Government to this agreement. In the absence of the specified notice, the

Government is not obligated to reimburse the Vendor for any costs in excess of the total amount allotted by the Government to this agreement, whether incurred during the course of the agreement or as a result of termination.

(i) When and to the extent that the amount allotted by the Government to the agreement is increased, any costs the Vendor incurs before the increase that are in excess of (1) the amount previously allotted by the Government or, (2) if this is a cost-sharing agreement, the amount previously allotted by the Government to the agreement plus the Vendor's corresponding share, shall be allowable to the same extent as if incurred afterward, unless the Agreements Officer issues a termination or other notice and directs that the increase is solely to cover termination or other specified expenses.

(j) Change modifications shall not be considered an authorization to exceed the amount allotted by the Government specified in the Schedule, unless they contain a statement increasing the amount allotted.

(k) Nothing in this article shall affect the right of the Government to terminate this agreement. If this agreement is terminated, the Government and the Vendor shall negotiate an equitable distribution of all property produced or purchased under the agreement, based upon the share of costs incurred by each.

(l) If the Government does not allot sufficient funds to allow completion of the work, the Vendor is entitled to a percentage of the fee specified in the Schedule equaling the percentage of completion of the work contemplated by this agreement.