



**Strategic & Spectrum Missions Advanced Resilient Trusted Systems (S²MARTS)
Request for Solutions (RFS)**

in support of

Core Based Threat Identification and Warning (I&W)

Project No. 22-07

A. OPPORTUNITY OVERVIEW

Project Title	Gray Summer: Core Based Threat Identification and Warning
Project Sponsor	Office of the Under Secretary of Defense (OUSD) for Research and Engineering (R&E)
Contracting Activity	Naval Surface Warfare Center (NSWC), Crane Division
Questions Deadline	May 23, 2022
Response Deadline	July 14, 2022
Anticipated Project Budget	\$15,000,000 (details below)
Resultant Award Type	Prototype Other Transaction Agreement (10 U.S.C. § 4022)

All respondents must be active NSTXL members.

B. PROTOTYPE PROJECT DETAIL

- Authority:** 10 U.S.C. § 4022, “Authority of the Department of Defense to Carry Out Certain Prototype Projects”
- Project Background & Current Capability:** The Office of the Under Secretary of Defense (OUSD) for Research and Engineering (R&E) Operate Through initiative seeks to identify, demonstrate, and assess capabilities that will provide solutions to operate through a wide range of Fifth Generation (5G) communication infrastructures. Recognizing the wide range of 5G architectures and their associated vulnerabilities, the general principle for all solutions are encouraged to operate through a zero-trust based architecture and technical approach.

The expanded technological capabilities of 5G introduce new means to compromise the security of Department of Defense (DoD) personnel that use connected devices. The DoD seeks tools that can be added at the Core Network to reduce the risk of exploitation throughout the 5G system, by either internal Managed Network Operator (MNO) network assets, peer networks (e.g., 3rd party or visitor networks) and/or rogue User Equipment (UE) devices that are operating on the network. While this initiative is focused on 5G technology, it is important to recognize and acknowledge the proliferation of Non-Standalone (NSA)

5G system deployments for the foreseeable future. Since the NSA architecture utilizes a 4G/Long-Term Evolution (LTE) Core (aka, Enhanced Packet Core or EPC) in conjunction with 4G and 5G Radio Area Networks (RAN) types, it is imperative that the resulting solutions can operate effectively on 4G/LTE systems, as well.

- Desired End-State & Success Criteria:** The DoD network operators need tools that provide insight into users on and methods for maintaining security across these 5G network infrastructures that are *under the cognizance of the Department of Defense*. As a part of the solution, DoD seeks to understand the threats and vulnerabilities that are introduced by 5G capabilities and methodologies to protect against those that would exploit them.

OUSD R&E envisions a solution that possesses the capability to provide network operators insight into anomalous behavior on the network according to their unique geographic setting and mission needs. This information is intended to provide the operator with enough information to make decisions and take action to maintain security of the network. In the second stage of this project, the solution should provide automated actions for anomalous behavior on the network, according to the characteristics of the unique setting and mission of the DoD personnel.

The solution must be capable of operating on both 5G Standalone (SA) and 5G Non-Standalone (NSA) networks; moreover, since the NSA architecture includes 4G/LTE system elements, this necessarily implies a requirement to operate on 4G networks, as well. This assumes that DoD personnel have access to the Core Network infrastructure in order to add/modify physical elements and/or add software updates. Solutions should consider and/or make use of existing solutions that are present in commercial Network Operation Centers (NOCs) and Security Operation Centers (SOCs), while retaining compliance with applicable standards and specifications. Proposed solutions should address as many of the below requirements and specifications as possible. Preferred solutions address all of the below requirements and specifications.

Specifications:

- The scope of required scanning is comprehensive, comprising all visible/identifiable elements including but not limited to: the local Core Network, remote locations of the same Core Network, and peer-Core Networks (e.g., through roaming partners, Managed Virtual Network Operator (MVNO) relationships, etc.); all RAN equipment, including assets that are managed by other MNOs as part of a RAN sharing arrangement; all 3rd party application servers residing in local or remote adjunct Data Networks; all Transport Networks that are employed to connect RAN, Core and Data Network equipment; and UEs of all types, including applications that utilize such UEs to facilitate communications.
- Anomalous behaviors are intended to be any behavior concerns observed by the network specific to DoD and would be analogous to the network health status which a mobile network operator is concerned with monitoring. Behavior may include activities such as overt attempts by unauthorized users to gain access to the network; authorized users to gain access to restricted network services or elements; repeated or abnormal attempts to request services or subvert commands from the network, etc.
- Applications must include a graphical user interface with control functions to allow both manual and automatic scanning and threat reporting.
- The dashboard should allow the network operator to customize the data displayed based on specific mission interests and location of mission operations.
- Threat monitoring and reporting must include independent selectable options for both local and remote operations.
- Solutions must be compatible with commercial off-the-shelf 5G 3rd Generation Partnership Project (3GPP) Rel 16 or later Core Network infrastructure equipment, as well as 4G Enhanced Packet Core (EPC) Network infrastructure that interoperates/interfaces with 5G 3GPP Rel 16 compliant RAN infrastructure (e.g., supporting 5G NSA deployments).
- Scanning must include spectrum monitoring functions in frequency bands applicable to the operator to discover threats or anomalous activities (e.g. out of band) impacting performance, confidentiality, integrity, and availability of the 5g network and its components.
- Scanning and response actions must not significantly reduce the performance, capacity or availability of the surveilled/monitored network elements, nor any of the corresponding applications that are running on them.
- Scanning solution must be compatible with 5G SA, 5G NSA, and 4G 3GPP compliant network architectures.

Prototype Attributes:

- Provide capability at the Core to reduce risk of information exploitation throughout the network. It should be assumed the Core and associated network are operated by a cooperative entity allowing for network appliance additions and modifications that do not otherwise negatively affect network performance or operations.
 - In conjunction with the Network Management System, the requested prototype continually scans authorized network elements (servers, routers, controllers, base stations, UEs, etc.) for degraded services and anomalous behavior such as security breaches, unauthorized network access, equipment compromise, etc.
 - Scan network for unauthorized network elements and provide capability to shut-down or isolate equipment.
 - Provide a graphical user interface and security dashboard which displays the security posture of the network and alert anomalous behaviors that might compromise the security of the network to the operator.
 - The dashboard should provide the operator with enough information pertinent to DoDs specified missions and provide insight to take actions in response to perceived threats.

Phased Approach:

Phase 1 will be a 6-month Period of Performance (POP). During this period there will be a kickoff, Technical Interchange Meeting (TIM), and a Preliminary Design Review (PDR). Prior to the end of Phase 1, each Awardee will develop and present a proposed, detailed plan related to how they expect to address Phase 2 prototype production, test, and evaluation efforts. A down-select is expected prior to Phase 2.

Phase 2 will be a 12-month POP with a Critical Design Review at month 8 and prototype demonstration and potential for a down select at month 12. During Phase 2, selected Awardees will begin the prototype production and test and evaluation process for transition.

Phase 3 will be a 6-month POP for continued transition, security assurance, and evaluation. Phase 1 and 2 may be conducted at any classification level, including unclassified. Performers interested in a Phase 3 award must obtain the appropriate clearance prior to the start of Phase 3.

For a prototype to be considered successful, the performer will conduct a Demonstration of the prototype on a DoD selected range facility in CONUS, during which the prototype's capabilities must be successfully demonstrated. For budget and planning purposes, proposals should assume the range facility will be a DoD provided range at Idaho National Laboratory. Range facilities may vary and will be determined as part of an award. A partial solution may be determined to be successful if the DoD determined it to be effective in a limited role. A Final Technical Report of the prototype capabilities as demonstrated at the Final Demonstration will also be required. Extended user evaluations or additional prototypes may be pursued to determine military utility.

4. Potential Follow-On Activity:

- a. Upon successful completion of this prototype effort, the Government anticipates that a follow-on production effort may be awarded via either contract or other transaction, without the use of competitive procedures if the participants in this transaction successfully complete the prototype project as competitively awarded from this document. The prototype effort will be considered successfully complete upon demonstration of the aforementioned technology objectives.
- b. Successful completion for a specific capability may occur prior to the conclusion of the project to allow the Government to transition that aspect of the prototype project into production while other aspects of the prototype project have yet to be completed.
- c. Requirements of other potential follow-on activities could involve, though not limited to, continued development and baseline management, fielding, sustainment, training, further scaling of the solution, integration of future capabilities, or integration of the solution with other capabilities.

5. Project Deliverables:

No.	Title	Description	Frequency	Delivery Method
1	Monthly Report	Program Status focused on Technical, Schedule, Budget	1/Month	Electronic
2	Program Kickoff	Kickoff	1	In person/ Virtual
3	TIM	Initial Technical Interchange Meeting	1	In person/ Virtual
4	PDR	Power Point or other briefing tools	1	In person/ Virtual
5	CDR	Hardware in the loop and Software in the loop Simulation and Power Point or other briefing tools	1	In person/ Virtual
6	Demonstration	Demonstrating on a DOD provided range (CONUS)	1	In person
7	Initial prototype Deliverables	<ul style="list-style-type: none"> Downloadable, licensed, and installable software packages Technical specifications and level-III software descriptions, application programming interface (API) specifications, and human readable source code. Installation and User manuals Necessary hardware 	1	Electronic delivery is preferred when possible. Hardware can be shipped.
8	Final Prototype Deliverable	<ul style="list-style-type: none"> Downloadable, licensed, and installable software packages Technical specifications and level-III software descriptions, application programming interface (API) specifications, and human readable source code. Installation and User manuals Necessary hardware 	1	Electronic delivery is preferred when possible. Hardware can be shipped.

Physical Deliverables should be shipped to:

COMMANDER
 ATTN Chris Parker BLDG 2038 CODE JXYS
 NAVSURWARCENDIV
 300 HIGHWAY 361
 CRANE, IN 47522-5001

6. Anticipated Budget

\$10-15M across awards

This value represents what is currently available for the subject project at the time of RFS release. This value is subject to change and is being provided for planning purposes only.

Respondents are encouraged to clearly explain how much of their solution can be developed for the advertised amount.

7. Anticipated Number of Awards

- The Government intends to award one (1) Firm Fixed Price (FFP) Other Transaction Agreement as a result of this RFS; however, more than one (1) award may be made if determined to be in the Government’s best interest. The Government reserves the right to not select any of the solutions proposed. The Government also reserves the right to execute fewer awards than anticipated, select aspects of a proposal for award, or not select any of the solutions proposed. The Government will collaborate with prospective awardees prior to finalizing the award.

- Partial responses addressing only a subset of the project's overall objectives are not permitted for this effort.

8. **Supporting Attachments & Links for Guidance:**

- a. Mandatory Section 889 Representation (Signature Required)
- b. DD254
- c. DD254 SCI Addendum
- d. DoD Program Manager Guidebook for Integrating the Cybersecurity Risk Management Framework in the System Acquisition Lifecycle ([https://www.dau.edu/tools/t/DoD-Program-Manager-Guidebook-for-Integrating-the-Cybersecurity-Risk-Management-Framework-\(RMF\)-into-the-System-Acquisition-Lifecycle](https://www.dau.edu/tools/t/DoD-Program-Manager-Guidebook-for-Integrating-the-Cybersecurity-Risk-Management-Framework-(RMF)-into-the-System-Acquisition-Lifecycle))
- e. Cybersecurity Test and Evaluation Guidebook (<https://www.dau.edu/cop/test/DAU%20Sponsored%20Documents/Cybersecurity-Test-and-Evaluation-Guidebook-Version2-change-1.pdf>)

C. SECURITY INFORMATION & RESTRICTIONS

1. This RFS, to include attachments, has been released in accordance with Distribution Statement A: Approved for public release.
2. Security classification & other restrictions:
 - Awardees/Prototype Level Performers are not required to possess an active facility clearance to perform in support of the subject project prior to response.
 - Compliance with International Traffic in Arms Regulation (22 C.F.R. §§ 120-130) is required no later than time of proposal.
 - The Performer shall have the ability to receive clearance for unescorted access to Government Owned Controlled Spaces. Access to TOP SECRET/Sensitive Compartmented Information (TS/SCI) will be for the purpose of required systems engineering and integration in support of Testing & Evaluation (T&E) at Government facilities. Further information pertaining to SCI policies and regulations is contained in the attached Contract Security Classification Specification DD-254.
 - The performer must have cleared key personnel that are approved or eligible for U.S. Government clearance at the appropriate level. Key performer personnel must possess required TS/SCI security clearances.
 - The offeror must state or demonstrate in their technical proposal their ability to meet the facility clearance/personnel security clearance requirements of the anticipated agreement. If the offeror does not currently have the clearance as required, they shall demonstrate their completion of the preparatory steps necessary to be granted a facility clearance within 180 days upon agreement award within their technical proposal.
 - The performer shall appoint a Security Officer who shall (1) be responsible for all security aspects of the work performed under this agreement, and (2) ensure compliance with any written instructions from NSWC Crane Security Officer.
 - Key performer and subperformer personnel assigned work under the agreement shall at a minimum be U.S. citizens and have a valid TS/SCI clearance as required.
 - The performer will require access to classified information systems when at Government locations. This includes access to the following classified information systems; SIPRNET and JWICS.
 - The performer will be required to have access to controlled facilities at Government facilities and/or other performer facilities in the execution of this tasking. The ability to receive, store, fabricate, modify, or generate classified information or material at the performer's own facility is not required.
 - The performer may require access to command/organizational email, web sites, portals, etc. The performer may also be required to obtain Common Access Card (CAC) badges as well as computer accounts such as NIPRNet, SIPRNet, and JWICS or equivalent systems.
 - The performer will require access to restricted data for the purpose of systems engineering, integration, and testing required in the performance of this agreement tasks and objectives.

- The performer will be required to have access to Controlled Unclassified Information (CUI) for the purpose of associated systems engineering, integration, and testing objectives required in the performance of this agreement.
- The performer will require access to foreign government information for the purpose of interfacing with NATO partners for the performance of this agreement in relation to systems engineering, integration, and testing in operational environment and scenarios.
- The performer will require access to NATO information for the purpose of interacting with NATO partners in support of agreement performance to include system engineering, integration, and testing in operational environments and scenarios.
- Performer will coordinate with OUSD R&E to perform any T&E events driven by classified operational environment/conditions/facilities/systems at appropriate Government facilities.
- The performer will generate, manage, and disseminate classified test reports or engineering artifacts through classified means in accordance with policies and regulations contained in the Contract Security Classification Specification DD-254.
- The Performer is required to protect critical information associated with this agreement to prevent unauthorized disclosure and will observe OPSEC requirements.
- The performer will require use of the Defense Courier Service for the transfer of classified material.
- By submitting a response, respondents shall certify whether covered telecommunications equipment or services **will or will not** be included as a part of its offered products or services to the Government in the performance of this effort. RFS Attachment A includes additional detail regarding the representation which must be signed and returned with any submissions.

What is included under “covered telecommunications equipment or services”?

- ✓ Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);
- ✓ 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);
- ✓ Telecommunications or video surveillance services provided by such entities or using such equipment; or
- ✓ 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.



1. All respondents/prospective performers must be compliant with the following:

- DoDI 8582.01, “Security of Unclassified DoD Information on Non-DoD Information Systems” and DODI 5200.48 “Controlled Unclassified Information.”
- NIST SP 800-171, “Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations”
- Research findings and technology developments arising from the resulting proposed solution 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 selected performer must comply strictly with the International Traffic in Arms Regulation (22 C.F.R. §§ 120-130), the National Industrial Security Program Operating Manual (DoD 5220.22-M) and the Department of Commerce Export Regulation (15 C.F.R. §§ 730-774).

D. DESIRED LEVEL OF DATA RIGHTS

Unlimited rights: The right to use, modify, reproduce, perform, display, release, or disclose technical data in whole or in part, in any manner, and for any purpose whatsoever, and to have or authorize others to do so.

E. PROCESS OVERVIEW & INSTRUCTIONS

1. Submission Process for Questions & Proposals

a. Questions


To submit any questions, visit the opportunities page at www.nstxl.org/opportunities, select the “Current” tab, locate the respective project, and select “Submit a Question”. Please refer to Page 1 for associated deadlines.

b. Proposals

To submit your proposal, visit the opportunities page at www.nstxl.org/opportunities, select the “Current” tab, locate the respective project, and select the “Submit Proposal” link. You must have an active account and be logged-in to submit your response.

Respondents are solely responsible for the timeliness of their submission and are cautioned that late submissions will not be accepted for evaluation. It is strongly recommended that interested parties submit their proposal as early as possible to uncover any potential technical or account issues. Please notify NSTXL immediately (membership@nstxl.org) if technical issues occur during the submission process and/or if confirmation related to membership status is required. Please refer to Page 1 for associated deadlines.

2. Proposal Structure & Assessment Methodology

	(1) Initial Review	>>>	(2) Follow-On Assessment	>>>	(3) Selection
ANTICIPATED TIMELINE*	Due: 07/14//2022, 12:00PM ET		Start of Follow-On phase: N/A		Award: 08/2022
TECHNICAL	Page Limit: 12 Format: MS Word and/or Adobe PDF		N/A		Award of Prototype Level Project
PRICE					

	<p>Page Limit: 5</p> <p>Format: MS Excel for pricing information; MS Word and/or Adobe PDF for supporting narratives</p>	N/A	
--	--	-----	--

**Anticipated dates are subject to change and are provided for planning purposes only.*

NSTXL will notify & invite Government-selected respondents to participate in a follow-on assessment/down select pending the outcome of the Government’s review of initial responses. Additional detail regarding the follow-on assessment will be provided at that time. Respondents who are not selected for follow-on assessments will also be notified of their status accordingly.

3. Format Detail

- a. 12-point font (or larger) for all response narratives; smaller type may be used in figures and tables but must be clearly legible.
- b. Page size of 8.5 x 11 inches.
- c. The following items are not included within the page count: Cover page, Table of Contents, supporting Foreign Owned, Controlled, or Influenced (FOCI) documentation, Section 889 Representation, and the Task Description Document (TDD) /Statement of Work (SOW).

4. Contents of Response (Cover Page, Technical Response, Price Response)

Proposal Cover Pages **must** identify the following:

- Company name
- Confirmation of active NSTXL Membership (e.g., “Verified NSTXL Member”)
Reminder: Contact membership@nstxl.org with any questions or requests for confirmation.
- Commercial and Government Entity (CAGE) Code (if available)
- Level of facility clearance (if available)
- Street Address
- Primary Point of Contact (with title, email address and phone number)
- Government Cognizant Security Office (CSO) responsible for monitoring the company’s National Industrial Security Program Standards compliance (with address, email address and phone number) If known
- Company’s security officer point of contact (with title, email address and phone number)
- All locations where work will be performed
- Business Size
- Business Type (Traditional or Non-Traditional)
- Status of U.S. ownership
- If the proposed approach requires any exceptions to this RFS
- If the proposed approach addressed all RFS objectives
- The applicable 10 U.S.C. § 4022 eligibility criteria (select **one** of the following)

- There is at least one nontraditional defense contractor or nonprofit research institution participating to a significant extent in the project;
- All significant participants in the transaction other than the Federal Government are small businesses (including small businesses participating in a program described under section 9 of the Small Business Act (15 U.S.C. § 638)) or nontraditional defense contractors; OR
- At least one third of the total cost of the project is to be provided by sources other than the Federal Government.



What is a nontraditional defense contractor?

An entity that is not currently performing and has not performed, for at least the one-year period preceding the solicitation of sources by the Department of Defense for the procurement or transaction, any contract or subcontract for the Department of Defense that is subject to full coverage under the cost accounting standards (CAS).

Review 48 CFR § 9903.201-1 for a list of CAS exemptions.

a. Technical responses must address the following topics:

TOPIC	INSTRUCTIONS
<p>Solution Narrative</p>	<ul style="list-style-type: none"> • Describe the approach used to design/deliver a unique prototype solution for the prototype technology objectives. • Include a discussion on schedule and the timing of all project deliverable(s) and other critical milestones. • Responses that only address a critical element of the total solution being sought, often referred to as a “partial solution”, must be clearly identified as such. • If the proposed approach will require exception to any aspect of this solicitation, to include attachments, respondents must clearly identify those exceptions within the Technical Volume of their response. All respondents are encouraged to review the baseline S²MARTS Performer’s Agreement available within the NSTXL Members Portal (nstxl.org).
<p>Team Overview</p>	<ul style="list-style-type: none"> • Identify each subperformer and include the following: <ul style="list-style-type: none"> - Summary of their role in support of the proposed concept - Commercial and Government Entity (CAGE) Code (if available) - Level of Facility Clearance (if available) - Address - Point of contact (with title, email address and phone number) - Business size - Business Type (Traditional or Nontraditional) - Status of U.S. ownership <p><i>Reminder: The responsibility to provide ample proof regarding nontraditional participation to a significant extent lies with the respondent and has a direct correlation to award eligibility.</i></p>

<p>Level of Data Rights Proposed</p>	<ul style="list-style-type: none"> The rights offered should be displayed in a manner that allows for ease of discussion in determining trade-offs and potential options for long-term sustainability of the deliverables of this effort. If rights are being asserted at a level less than the Government’s desired level, respondents must provide detail explaining the specific rationale for the assertion. Any items previously developed with federal funding (and utilized in support of the proposed solution) should clearly identify all individual components funded by the Government and the recipient of the deliverables. If commercial software is proposed as part of the prototype solution, all applicable software licenses must be identified and included with the response. Note that any software license term or condition inconsistent with federal law will be negotiated out of the license.
<p>Explanation Supporting Eligibility for Award of a Prototype OTA</p>	<ul style="list-style-type: none"> Provide rationale to support the specific eligibility condition that permits award of an Other Transaction to the proposed performer/team. The responsibility to provide ample proof regarding <i>nontraditional defense contractor participation to a significant extent; small business or nontraditional defense contractor status; or any cost sharing arrangement</i> lies with the respondent and has a direct correlation to award eligibility. <p style="text-align: center;"><u>Questions regarding eligibility?</u></p> <p>Contact NSTXL and/or review 10 USC 4022 and the DoD Other Transaction Guide for additional information.</p>
<p>Foreign Owned, Controlled, or Influenced (FOCI) Information (if applicable)</p>	<ul style="list-style-type: none"> Identify if the primary performer and/or any sub-performers (to include vendors, suppliers, subcontractors, and teaming partners) are considered under FOCI. <p style="text-align: center;"><u>Supporting documentation may include but is not limited to:</u></p> <p style="text-align: center;">Standard Form 328 (Certificate Pertaining to Foreign Interest); Listing of Key Management Personnel; an Organizational Chart; Security Control Agreements: Special Security Agreements; and Proxy Agreements or Voting Trust Agreements.</p>
<p>Government Furnished Support</p>	<ul style="list-style-type: none"> Identify if the proposed solution will be dependent on Government Furnished Property (GFP) or other forms of Government support (i.e. information, schematics, laboratory, or facility access). If the solution is dependent on the Government furnishing specific information or items, describe the impact to the solution if the request cannot be met. All GFP proposed and/or required for the respondent to perform this effort shall provide documentation that the proposed Government property usage has been approved by the cognizant Contracting Officer or Agreements Officer.
<p>Compliance</p>	<ul style="list-style-type: none"> Respondents must address each mandatory restriction/requirement identified within this RFS and explain how each regulation or standard is currently, or will be met. <p style="margin-left: 40px;">✓ Note: If exceptions to any of the restrictions/compliance requirements exist, respondents must fully explain the basis for the exception and how any correlating risk will be mitigated.</p>

	<ul style="list-style-type: none"> In addition to the mandatory representation included as Attachment 1, respondents must include the following statement within the Compliance section (with the applicable answer checked): “[Company Name] represents that 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.” ✓ Note: If your company will provide covered telecommunications equipment or services, please contact S2MARTS@nstxl.org for additional mandatory disclosures that must be completed & submitted with your response (at least 72 hours in advance of the response deadline).
Organizational Conflicts of Interest	<ul style="list-style-type: none"> All responses must disclose and address potential conflicts of interest and any proposed mitigation. If OCI's are not present, respondents must include a statement within the Technical Volume that no OCI's are present.
Task Description Document/ Statement of Work	<ul style="list-style-type: none"> Provide a Task Description Document (TDD) outlining the project tasks to be performed along with schedule milestones and delivery dates required for successful completion. It is anticipated that, if selected, the proposed TDD will be incorporated into the resultant prototype-level Project Order, similar to a Statement of Work (SOW). Respondents are encouraged to be concise but thorough when outlining their TDD/SOW. The TDD/SOW may be submitted as an appendix or a separate file as part of the proposal.

5. Contents of Pricing Response

Note: The Government reserves the right to seek additional detail related to pricing if a conclusive fair & reasonable determination cannot be achieved. Respondents are encouraged to provide thorough & detailed responses (to the maximum extent practicable) to reduce likelihood of schedule delays and increase the Government's understanding of the proposed concept.

TOPIC	INSTRUCTIONS
Price Breakdown	<ul style="list-style-type: none"> Delineate key pricing components and show clear traceability to the phases and/or milestones of the Technical Response. At a minimum, key pricing components include: <ul style="list-style-type: none"> Labor Total(s), Other Direct Costs/Material Total(s), any license prices/fees, and subcontractor/vendor/sub-performer price(s). Data should be organized & clearly identified by technical objective, milestone, and/or phase proposed (if phasing is applicable).
Supporting Narrative	<ul style="list-style-type: none"> Include a brief narrative that explains your pricing structure and maps the proposed prices to the solution's technical approach.
Payable Milestone Schedule	<ul style="list-style-type: none"> The overall total price should be divided among severable increments that align to a proposed milestone payment schedule. Milestones are not required to match actual expenditures but should realistically align to the effort expended or products delivered.
Innovation & Scalability (if applicable)	<ul style="list-style-type: none"> Any additional features or beneficial capabilities that extend beyond the currently requested technical objectives shall be separately priced for the Government's consideration.

Price Impacts of Data Assertions <i>(if applicable)</i>	<ul style="list-style-type: none"> If limited or restricted rights are being asserted within the response, provide a table that includes prices if the Government elects to purchase increased level of rights.
Supporting Information	<ul style="list-style-type: none"> Inclusion of supporting information, such as a Basis of Estimate, may substantially expedite evaluation of your response.

F. Solution Review & Assessment

Compliant responses will be evaluated with consideration given to:

**Demonstrated understanding and overall technical merit of the response;
Feasibility of implementation; and,
Total project risk (related to technical focus areas, price, schedule and/or compliance)**

- The Government will evaluate the degree to which the proposed solution provides a thorough, flexible, and sound approach in response to the prototype technical objectives. While the technology objectives are of significant importance, responses will be considered as a whole.
- The Government will select the prototype-level performer and award this project, via NSTXL, to the respondent(s) whose solution is assessed to be the most advantageous to the Government, when price, schedule, technical potential, level of data rights, and other factors are considered. The Government reserves the right to award to a respondent that does not meet all the requirements of the RFS.
- The Government reserves the right to reject a submission and deem it ineligible for consideration if the response is incomplete and/or does not clearly provide the requested information.
- Debriefings will not be provided.

G. Additional Project Information

- The Government intends to award one (1) FFP Other Transaction Agreement as a result of this RFS; however, more than one (1) award may be made if determined to be in the Government's best interest. The Government also reserves the right to not select any of the solutions proposed.
- Acceptable responses not selected for the immediate award will be retained by NSTXL & the Government for possible future execution and funding. The non-selected proposals will be considered as viable alternatives for up to 36 months. If a proposal (that was not previously selected) is determined to be a suitable alternative, the company will be contacted to discuss any proposal updates and details of a subsequent project award.
 - Respondents whose proposals are not selected for the initial award shall not contact the Government or NSTXL to inquire about the status of any ongoing effort as it relates to the likelihood of their company being selected as a future alternative.
- The United States Navy, specifically Naval Surface Warfare Center, Crane Division, maintains release authority on any and all publications or press releases related to this prototype project.
- Unsuccessful respondents will be notified by NSTXL, however, debriefings for this project will not be provided.
- Certain types of information submitted during the RFS and award process of an OT are exempt from disclosure requirements of 5 U.S.C. §552 (the Freedom of Information Act or FOIA) for a period of five years from the date the Department receives the information. It is recommended that respondents mark business plans and technical information that are to be protected

for five years from FOIA disclosure with a legend identifying the documents as being submitted on a business confidential basis.

- No classified data shall be submitted within the proposal. To the extent that the project involves DoD controlled unclassified information, respondents must comply with DoDI 8582.01 and DoDM 5200.01 Volume 4. Respondents must implement the security requirements in NIST SP 800-171 for safeguarding the unclassified internal information system; and must report any cyber incidents that affect the controlled unclassified information directly to DoD at <https://dibnet.dod.mil>.

- This is to advise that non-Government advisors will assist in the evaluation. The use of non-Government advisors will be strictly controlled. Non-Government advisors will be required to sign a Non-Disclosure Agreement (NDA) prior to working on the effort. Agreements Officer will review NDAs for conflict prior to allowing access to source selection information. All non-Government advisors will only have access to the information corresponding to their area(s) of expertise. Advisors will not have access to the Price Volume of the response. The companies identified herein have agreed to not engage in the manufacture or production of hardware/services/research and development that is related to this effort, and to refrain from disclosing proprietary information to unauthorized personnel.
 - The following companies will have non-Government personnel advising:
 - Avantus Federal, LLC, 8281 Greensboro Dr STE 400, McLean, VA. Cage Code: 36KWO
 - Catalina Associates, LLC., 2107 Eden Woods Ln. Gambrills, MD. Cage Code: 804V3
 - Disruptive Technology Associates, LTD., 621 E Goldenrod St. Phoenix, AZ. Cage Code: 78LV4
 - University of Maryland, 2103 Reckord Armory, College Park, MD. Cage Code: 3HEM3