STRATEGIC & SPECTRUM MISSIONS ADVANCED RESILIENT TRUSTED SYSTEMS (S²MARTS)

REQUEST FOR SOLUTIONS (RFS)
in support of the
SUPPLY CHAIN AWARENESS TOOL PROTOTYPE PROJECT
PROJECT NO. S2MARTS19-01

1. Requiring Activity/Project Sponsor Seeking Solution

Naval Surface Warfare Center (NSWC) Crane Division in support of the Office of Secretary of Defense (OSD) for Microelectronics Innovation for National Security & Economic Competitiveness (MINSEC).

2. Background (Current State of Technology)

Department of Defense (DoD) programs rely heavily on commercial microelectronics to maintain a technological advantage over the adversary. This reliance on commercial hardware has resulted in a dramatic decline in visibility of critical supply chains. Current DoD and industry standards provide a shallow view of device supply chains that focus heavily on risks associated with the device intellectual property (IP) owner, rather than the third party manufacturing structure that is responsible for the majority of semiconductor production. Unique devices produced by the same company may have wildly different supply chains, and associated risks.

The process identified in the Supply Chain Awareness Reporting Overview, Attachment 1, is conducted manually and tracked on a spreadsheet. Queries currently take approximately 80 hours to complete. Aggregate data is collected and maintained for part-centric supply chain risk management.

3. Description of Need (Critical Capability Gaps)

The Navy is pursuing a prototype in order to develop a part-centric supply chain awareness tool. Supply Chain Risk Management (SCRM) is the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of product and service supply chains. The purpose of this prototype is to facilitate the identification portion of SCRM and how it could be used as input for a more in depth supply chain assessment. The supply chain awareness tool identifies critical nodes in design, production and distribution when a product may be susceptible to malicious insertions, inferior substitutions, supply interruptions, or IP theft.

Proactive supply chain awareness and security is a key element in the success of NSWC Crane programs. As part of these programs, a part-centric supply chain tool will be developed that will determine the supply chain risk of specified microelectronic components so that DoD programs can make more informed decisions on selection of components for system design and overall acquisition process. Achieving the objective will require novel and unique methods including but not limited to: identifying sources of data for ingestion, tool design and development, identifying and establishing risk categories, and determining statistical factors and data that aid in risk determination.

The desired outcome will utilize machine learning to develop, demonstrate, and exploit technologies, algorithms, and methods that expand the ability of a computer to learn from data, other computers, or sensors, without human intervention. Machine Learning computers can improve themselves from data, knowledge, experience and interaction with other computers. A computer with machine learning capabilities may use elements of statistics, knowledge science, computer science/systems, natural language processing, large database construction and management, and planning and control to improve its ability to suggest or predict outcomes of situations. In the prototype solution, the goal will be an implementation of these capabilities, possibly in a phased approach, to attain a more consistent and automated method for identification of numerous part types with regard to authenticity. Modeling and Simulation may be used to develop and demonstrate the prototype throughout the project and may include virtual and augmented reality.

NSWC Crane seeks a prototype that will employ machine learning, Artificial Intelligence (AI), web scraping and other methods to ingest data on parts and companies, evaluate and prioritize that data, present it to the analyst in fashion that allows rapid and accurate analysis, and aggregate and visualize data in a way that provides the end user with a clear understanding of risks associated with single devices and compound risk associated with collections of devices (Circuit Card Assemblies, Lowest Replaceable Units, Systems, etc.). The current process is largely manual and requires significant time investment from an analyst to collect and aggregate relevant data, requiring approximately 80 hours per device. Currently, demand for this service dramatically outstrips supply. While it will likely never be possible to remove analysts from the process, much of the source data is available via open source or subscription services, that could be ingested using automated methods.

There is a need to minimize the amount of time it takes to do a query on semiconductor devices, and to minimize the amount of subjective prioritization of data that is intrinsic to manual data collection. Currently, it takes approximately 80 hours to complete a query that compiles the necessary information to determine the risks associated with a part.

It is desired that initial development will generate a proof of concept, basic architecture models, and an evaluation of existing data sources and associated costs. With the following development focused (as a minimum) on leveraging these deliverables to develop a functional prototype capable of ingesting data and providing analyst visualization of selected data sources with potential extended development focusing on web-scraping, AI, machine learning to improve data collection and analyst decision making, and employing data analytics methods to identify compound risks that can be identified in the broader data set.

The prototype efforts will use existing Department of Defense Architecture Framework (DoDAF) compliant architecture models and ensure cybersecurity compliant systems that drive obtaining authority to operate (ATO) approvals after completion of the prototype. Preference is for this tool to be Common Access Card (CAC) enabled to add additional layers of secure access.

DoDAF Models and Descriptions can be found at: https://dodcio.defense.gov/Library/DoD-Architecture-Framework/dodaf20_models/

DoDAF Version 2.02 can be found at: https://dodcio.defense.gov/portals/0/documents/dodaf/dodaf_v2-02_web.pdf

4. Prototype Technology Objectives (End State Success Criteria)

The end state goal is to meet the technology objectives indicated below. Respondents that propose partial solutions will be reviewed and considered. Respondents may also propose additional capabilities/enhancements for consideration.

(a) Automated query process and reduced query time to less than 80 hours without losing any visibility into existing data sets.

(b) Identifies the critical data sources (and associated cost) required to fully map an integrated circuit's life cycle, from design through its end-of-life. This process conveys an understanding of an integrated circuit's supply chain, it exhibits the ability to understand where risks are throughout that life cycle, and an understanding of where and how to obtain information on an individual component's life cycle.

(c) Demonstrates the ability to perform automated data ingestion and link all of the data, particularly unstructured data sources, and conduct entity resolution.

(d) Leverages application program interfaces (APIs) and data-scraping wherever possible to automate data collection, and data sets that cannot be automated will have an associated import wizard that allows the rapid ingestion of manually collected data in its native format without significant manual manipulation.

(e) Utilizes Data Analytics, Artificial Intelligence and/or Machine Learning in areas of data ingestion, entity resolution, and risk determination.

(f) Demonstrates how the combination of data on individual components and companies can lead to a data graph database with a corresponding network diagram depicting the complex relationship network of corporate entities, persons of interest, and individual devices to illustrate high risk supply chain nodes and aggregate risks such as recurring exposure to high risk regions or entities, health of sectors, and product availability issues within the semiconductor industry.

(g) Offers equivalent or improved data quality for each data item versus the original manual process as shown in Attachment 1.

(h) Supports full device centric supply chain evaluation that is sufficiently granular to allow the user to identify specific supply chain sites associated with different devices from the same manufacturer, different lots of the same devices, and similar devices from different manufacturers.

(i) Will consist of a software development package capable of accommodating all proposed features.

(j) Addresses potential hosting options and identifies multiple viable sources compliant with the selected software architecture.

(k) Prototype will need to be capable of accreditation for ATO approval in accordance with DoD cybersecurity requirements. ATO will be attained by the Government after the tool has been proven to ensure it can meet objectives. (Reference: NIST 800-37 & NIST 800-53)

5. Funding Profile

(a) This project is currently budgeted at $2,500,000. Respondents may propose additional benefits and capabilities above and beyond the stated objective for consideration and potential additional funding.

6. Deliverables

Description (Reports / Items)	Frequency	Due Date
DoDAF Architecture Diagrams	One (1)	To Be Delivered when Completed*
Software Package	One (1)	To Be Delivered upon completion of the Prototype
Accreditation Test Package	One (1)	Upon Completion of the verification and validation of the Test Package
User Guide	One (1)	To Be Delivered upon completion of the Prototype
3rd Party License Agreements Documentation	As required	Prior to Procurement of each license agreement.**

**Will be finalized at contract award.*

*** Verification of third party licenses are needed. The Government desires awareness of and concurrence with any and all third party agreements.*

7. Level of Data Rights Desired by Government

Government Purpose Rights: The right to use, modify, reproduce, release, perform, display, or disclose technical data within the Government without restriction. This also includes the rights to release or disclose technical data outside the Government and authorize persons to whom release or disclosure has been made to use, modify, reproduce, release, perform, display, or disclose technical data for United States government purposes. This level of restriction is set at five-years but may be negotiated & tailored to a specific project. The five-year period, or such other period that may be negotiated, would commence upon execution of the agreement that required development of the items, components, or processes or creation of the data. The performer will have the exclusive right, including the right to license others, to use technical data in which the Government has obtained government purpose rights under this agreement for any commercial purpose during the five-year period. Upon expiration of the five-year period (or other negotiated length of time), the Government will receive unlimited rights in the technical data and computer software.

8. General Information

Vendors are solely responsible for all expenses associated with responding to this Request for Solutions. Evaluation and selection of the solution(s) will be completed based on the criteria in Paragraphs 9 and 10 below. Funding for this project is currently available. NSWC Crane intends to competitively issue this effort as an Other Transaction Agreement (OTA) in accordance with 10 U.S.C. 2371b. If an OTA is awarded from this request, the Agreement is not considered a procurement contract and therefore is not subject to the Federal Acquisition Regulation. The following general formatting requirements apply:

- Times New Roman Size 10 font (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).
- Please note that 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.
- Files must be submitted electronically in PDF and/or Microsoft Word formats only.

9. Contents and Format of Response

(a) Section 1: Technical Solution and Approach (Page Limit: 15 Pages)

i) Cover Page: The cover page does not count in the 15-page limit. The cover page shall include the company's name, Commercial and Government Entity (CAGE) Code (if available), level of facility clearance (if available), address, primary point of contact, and status of U.S. ownership.

On the cover page, please identify the applicable 10 U.S. C. § 2371b eligibility criteria being met (please identify only one):

- 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.

- At least one third of the total cost of the project is to be provided by sources other than the Federal Government.

  Nontraditional Defense Contractor is defined as 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 (DoD) for the procurement or transaction, any contract or subcontract for the DoD that is subject to full coverage under the cost accounting standards prescribed pursuant to 41 U.S. Code § 1502 and the regulations implementing such section.

ii) Technical Response:

(1) Solution Narrative: Respondents shall describe the approach used to deliver a unique prototype solution for the prototype technology objectives defined in Section 4 of this RFS. While these focus areas are of significant importance, responses will be considered as a whole. Respondents may propose features and capabilities for consideration above and beyond the current technical objective. Proposed additional features or capabilities can be added as an attachment to the proposal and will not be included in the page count.

(2) Government Furnished Property or Information: Within the technical response, respondents must clearly identify if its proposed solution depends on Government Furnished Information (GFI) / Government Furnished Property (GFP).

If so, the response must specify the GFI / GFP required. If the solution is dependent on GFI / GFP, the Government will determine whether the GFI/GFE can be provided, the impact to the solution if the requested information/property is not available, and will confirm the details with the respondent prior to any proposal revisions or selection, if applicable.

(3) A Statement of Work (Not Included in Page Count) outlining the tasks required along with schedule milestones and delivery dates is requested for successful completion. It is anticipated that, if selected, the proposed Statement of Work will

be incorporated into the resultant OTA. Respondents are encouraged to be concise but thorough when outlining their work statements.

(4) Summary of Subcontractor Participation (if applicable):

(a) Provide a list of all subcontractors involved and their role within the performance of the proposed concept. If their involvement is considered significant, ensure the rationale is present within the narrative. The onus of proof to support participation to a significant extent or any cost sharing arrangement lies with the respondent.

(b) Provide the subcontracting company's name, Commercial and Government Entity (CAGE) Code (if available), level of facility clearance (if available), address, primary point of contact, and status of U.S. ownership. Foreign Owned, Controlled, or Influenced (FOCI) Mitigation Documentation shall be provided for subcontractors, if applicable, and will not count towards the page count.

(5) Data Rights Assertions and Level of Rights Proposed:

(a) 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.

(b) If limited or restricted rights are being asserted within the response, detail supporting the specific rationale for this assertion must be included.

(c) Any items previously developed with federal funding should clearly identify all individual components funded by the Government and the recipient of the deliverables.

(d) 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.

(e) Restricted rights apply only to noncommercial computer software and has the meaning included in Defense Federal Acquisition Regulation Supplement 252.227-7014(a)(15).

(f) It is recommended that the proposal consider the rights desired by the Government as identified within Request for Solution, Section (8), Level of Data Rights Desired by Government.

(6) Foreign Owned, Controlled, or Influenced (FOCI) Mitigation Documentation (if applicable): Documentation may include, but is not limited to: 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. It is recommended that companies who fall within the FOCI category visit https://www.dss.mil for additional guidance and instruction.

(b) Section 2: Price (Page Limit: 5 Pages)

i) Price Cover Page: The price response shall be submitted as a separate document from the technical response. No pricing details shall be included in the technical response.

ii) Pricing Breakdown:

(a) Respondents shall propose a Fixed Price for the proposed solution. The overall total price should be divided among severable increments that align to a proposed milestone payment schedule.

(b) In order to support the Government's evaluation of fair and reasonable pricing, the respondent shall delineate the key pricing components, and show clear traceability to the technical narrative and focus areas and phases described by the Government. At a minimum, key pricing components include Labor Total(s), Material Total(s), and Subcontractor price(s). Each should be outlined for each focus area and/or phase.

(c) If limited or restricted rights are being asserted within the response, a table that prices both Government Purpose Rights and Unlimited Rights for any such limited or restricted item must be included.

(d) This shall include estimated costs for initial architecture development and outline the associated cost of future developments to add capability. Outline any labor, material, other direct costs, or sub-contracts.

(e) Any additional benefits from the core solution shall be separately priced. Any additional features or capabilities above the technical objective for consideration.

10. Selection Criteria & Methodology:

(a) Individual responses will be evaluated with consideration given to:

i) Demonstrated expertise and overall technical merit of the response;
ii) Feasibility of implementation; and
iii) Total project risk as it relates to the technical focus areas, price and schedule

The Government will evaluate the degree to which the submission provides a thorough, flexible, and sound approach in response to the prototype technical objectives as stated in Section 4 of this RFS as well as the ability to fulfill the requirements in RFS.

The Government will award this project, via S^2MARTS (Agreement No. N00164-19-9-0001), to the respondent(s) whose solution is assessed to be the most advantageous to the Government, when price, schedule, technical risks, the 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 assessment of risks is subjective and will consider all aspects of the proposed solution. Respondents are responsible for identifying risks within their submissions, as well as providing specific mitigating solutions.

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.

11. Follow-On Production

(a) Upon successful completion of this prototype effort, the Government anticipates that a follow-on production effort may be awarded via either contract or transaction, without the use of competitive procedures if the participants in this transaction successfully complete the prototype project as awarded from this document. The prototype effort will be considered successfully complete upon delivery of a prototype that meets the identified technical 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, sustainment, further scaling of the solution, integration of future capabilities, or integration of the solution with other capabilities. For planning purposes, follow-on production of the subject capability may include the following outcome(s): Fielding & Sustainment across multiple DoD activities.

12. Response Due Date

Responses are due **no later than 2:00PM Eastern Time on May 06, 2019** and shall be submitted via email to initiatives@nstxl.org. Email subject lines must include **S2MARTS19-01**.

13. RFS Attachments

(a) Attachment 1 - Supply Chain Awareness Reporting Overview

14. Additional Information & Disclaimers

(a) The Government intends to award one Other Transaction Agreement as a result of this Request for Solutions; however, more than one 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.

(b) Acceptable responses not selected for the immediate award will be retained by the Government for possible future execution and funding. The non-selected proposals will be considered as viable alternatives for up to 24 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 Consortium Manager to inquire about the status of any ongoing effort as it relates to the likelihood of their company being selected as a future alternative.

(c) The United States Navy has release authority on any publications related to this prototype project.

(d) If resource-sharing is used, in accordance with 10 U.S. Code § 2371b(d)(1)(C), then the non-Federal amounts counted as provided, or to be provided, by parties other than the Federal Government may not include costs that were incurred before the date on which the OT agreement becomes effective. Costs offered as a resource-share that were incurred for a project after the beginning of negotiations, but prior to the date the OT agreement becomes effective, may be counted as non-Federal amounts if and to the extent that the Agreements Officer determines in writing that: (1) the party other than the Federal Government incurred the costs in anticipation of the OT agreement; and (2) it was appropriate for the entity to incur the costs before the OT agreement became effective in order to ensure the successful implementation of the OT agreement.

(e) Certain types of information submitted to the Department in a process having the potential for award 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.

(f) 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.

(g) Export controls: 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).