Prototype Acquisition Approach (PAA)

in support of

Rapid Assured Microelectronics Prototypes using Advanced Commercial Capabilities (RAMP)

PAA PART 1

Part 1 outlines the statutory eligibility, funding data, and overall intent of the subject project.

It is anticipated that a Project Order (PO) or multiple POs, will be issued under the Terms and Conditions outlined in the base agreement, N00164-19-9-0001. Any PO awarded under the terms and conditions of the base agreement will be in accordance with 10 U.S. Code § 2371b and the Office of the Under Secretary of Defense of Acquisition and Sustainment Other Transactions Guide, Version 1.0 – November 2018.

1. Prototype Eligibility Review and Approval

1.1. Project Title & Acronym: Rapid Assured Microelectronics Prototypes using Advanced Commercial Capabilities (RAMP)

1.2. Requiring Activity: Naval Surface Warfare Center, Crane Division, Trusted Microelectronics Division (GXV)

1.3. Contracting Activity: Naval Surface Warfare Center, Crane Division, Code 0221

1.4. Estimated Ceiling & Approval Level

Estimated Project Ceiling: $85,000,000

Approval Level: < $75M (NSWCC Agreements Officer)

1.5. Funding Type and Amount

Fiscal Year 20XX	Amount	Appropriation	Sponsor(s)
19	$50,000,000	Research, Development, Test & Evaluation (RDT&E)	Office of Secretary of Defense (OSD) Research and Engineering (R&E)

20	$35,000,000	Research, Development, Test & Evaluation (RDT&E)	Office of Secretary of Defense (OSD) Research and Engineering (R&E)
21	$		
22	$		
Total	$		

1.6. Problem Statement, Area of Need, or Capability Gap

1.6.1. Background:

The United States Navy and Air Force, in support of the Office of the Secretary of Defense (OSD), is developing integrated circuit (IC) hardware and workflow prototypes that promote the use of assurance principles, feature protections, and correlation. The purpose of this prototype is to facilitate the rapid development of IC hardware for further evaluation and technology enablement of DoD, while simultaneously generating workflow prototypes using commercial best practices for DoD Defense Industrial Base (DIB).

The RAMP prototype project addresses brand new technology development that will provide DoD relevant IC prototypes utilizing advanced node fabrication that mitigate the need for International Traffic in Arms Regulations (ITAR) fabrication. Rapid generation and assurance of microelectronic systems is directly relevant to enhancing the mission effectiveness of military personnel and the supported platforms, systems, and components acquired or developed by the DoD and enables assured microelectronics to be used by the services.

In support of this need, the Navy and Air Force desire to leverage commercial capabilities to develop a RAMP prototype methodology to demonstrate secure enhanced design utilizing commercial fabrication processes for DoD's programs. The emphasis on physical design refers to the post Registered Transfer Level (RTL) portion of design that includes automated place and route, timing closure, and verification of the physical design. Physical design is particularly challenging because the design methods used are tightly coupled with specific fabrication processes and facilities and because physical design has become more and more complex as semiconductor processes have become more advanced.

The primary objective of the project is to leverage the expertise of commercial industry to develop and demonstrate a novel capability for design of State-of-the Art (SOTA) (defined as $\leq$ 22nm node Si CMOS) ICs and System On a Chip (SoCs) microcircuits that can be designed and verified in the most advanced semiconductor processes. In addition, a RAMP prototype will achieve lower power consumption, improved performance, reduced physical size, and improved reliability for application in DoD systems. It is important to

note that this prototype supports, but does not directly address Packaging or Radiation Hard circuit design. These areas are addressed by other DoD programs.

Achieving the objective will require novel and innovative methods including unique and secure design tools and critical circuit modules required to design advanced custom ICs and SoCs. Secure IC and SoC design resources will also be developed to support successful demonstration of the RAMP prototype. This objective also requires a complex IP licensing and support model, and close fab relationships

1.6.2. Current State of Technology:

The RAMP project intends to address and replace the obsolete practices utilized by the United States Government in support of SOTA custom IC and System On a Chip (SoC) design, especially those associated with physical or "back-end" design. These current, outdated processes have resulted in the effectiveness of the Department of Defense (DoD) and the traditional Defense Industrial Base (DIB) being significantly superseded by commercial industries and other non-DoD markets in the design and fabrication of SOTA ICs and SOCs.

1.7. Desired End-State Technical Objective(s) and Success Criteria

The initial project award will encompass Phase 1, Establishment of a Prototype IC and SoC Secure Design Capability, that emphasizes Physical Design capability and should support implementation of export-controlled DoD designs through use of protection technologies. Subsequent phases, Phase 2 (Demonstration of Prototype Designs Using the IC and SoC Physical Design Infrastructure) and Phase 3 (Validation of Designs Using the IC and SoC Physical Design Infrastructure) may be funded and executed upon successful completion of Phase 1. Successful completion of Phase 1 will be measured via the metrics identified within the Deliverables table below.

The Navy and Air Force desires secure IC and SoC physical design solutions that will support advanced prototype development to drive innovation in design of advance digital and mixed-signal integrated circuits and their use to drive innovation in DoD systems. The Phase I objective will be achieved through three major task:

1. Establishment of Secure Design Capability that supports and enhanced physical design by the Defense Industrial Base (DIB) in SOTA (defined as ≤ 22nm node Si CMOS) technology nodes.
2. Application of methods to ensure both the confidentiality and integrity of circuits during the manufacturing flow.
3. Definition of a DoD supply chain standard that leverages commercial microelectronics supply chain security methods to meet DoD needs.

Each of these tasks are be described in more detail below:

1. Secure Design Capability

This task will establish one or more secure design capabilities that facilitate rapid implementation of DIB digital and mixed-signal designs in SOTA (<22nm) CMOS technologies. Each capability should define optimal design flows and engineering support mechanisms to dramatically enhance the ability of the DIB to securely design and realize SOTA ICs and SoC technology. Each design capability will utilize infrastructure that supports the collection of a standard set of assurance data during the design process. Each design capability must have resident expertise and demonstrated experience with advanced technology (≤ 22nm) design, physical implementation, and fabrication. Each design capability will have fabrication facility specific implementation knowledge to ensure the ability to effectively represent requirements, guide, and support DIB design teams through the release to manufacturing process. The expectation is that each design capability will strongly leverage commercial expertise in physical design at SOTA technology nodes to achieve these goals. Each design capability must also be supported through a strong business plan for maintaining the capability during and after funding for the RAMP project is completed. It is preferred that the Secure Design Capability does not lead to a closed security implementation and is not tied to a single fabrication facility/flow.

2. Methods to Ensure Confidentiality and Integrity of ICs/SoCs

This task will apply the best known methods, including government sponsored and commercially developed, for ensuring confidentiality and integrity of integrated circuits through the fabrication process. Confidentiality is defined as the protection of sensitive design information during the implementation and manufacturing process. Integrity is defined as the quantified assurance that both the front end and back end of microelectronics fabrication are performed as expected with no unanticipated or un-attributable alterations of the design during the manufacturing process. This task will support implementation of export-controlled DoD designs in commercial foundries through the application of protection technologies. This task should demonstrate the ability to leverage fabrication knowledge to ensure confidentiality/integrity is effectively implemented for DIB designs and preserved throughout transformations that occur in the release to manufacture process.

3. DoD Supply Chain Security

Phase I of this task will focus on leveraging best practices of commercial microelectronics supply chain security methods. This task will define ways to leverage commercial supply chain security methods to meet DoD needs and are compatible with commercial

manufacturing practices.

This task will focus on the establishment of a standard set of assurance data that will provide the quantitative evaluation of the security, confidentiality and integrity of the IC and SoC design/fabrication supply chain. It is expected that performers will heavily leverage existing, commercial sources of data such as those used for ensuring safety critical and high reliability systems. Where additional data is required to meet DoD needs, collection of this data will be compatible with commercial design and manufacturing practices. This task will include a recommended draft set of design standards with input from the Government Technical team, as needed.

These three tasks will support the overall goal of the RAMP program to greatly enhance the capability of the DIB to securely design SOTA IC and SoC designs that will support advanced prototype development and drive innovation in design of advance digital and mixed-signal SoCs. This enhanced capability will increase SOTA IC and SOC use by the DIB and drive innovation in DoD systems.

Phase 2 Objectives:

Phase 2 will be a continuation of tasks 1 and 2 as well as the demonstration of the secure design capability and implementation of quantifiable assurance technology by utilizing them to design and build DoD relevant designs in coordination with the DIB.

Phase 2 will demonstrate the implementation of the capabilities developed in tasks 1 and 2 by exercising the design, fabrication, and will be required to test at least three DoD relevant Designs. At least one must be a SOC that incorporates commercial and DoD application specific IP, one must be a Digital IC and the third must be a mixed-signal IC that will be selected in coordination with the DoD evaluation team. The demonstration ICs should be designed by the DIB and should span a wide range of physical design support models from support-only (Foundry Flow) to turn-key physical design (ASIC Flow) by the design capability. Each demonstration IC design will include techniques to ensure Confidentiality and Integrity are preserved during fabrication in the commercial SOTA foundry. The task will conduct an independent assessment of the techniques and resulting demonstration articles. The demonstration articles will be provided to the government with all necessary information to conduct a government led evaluation. The design capability should provide to the government a standard set of assurance data, with provenance and traceability, created by EDA tools during the integrated circuit design process: 3rd party IP sources, tools, scripts, versions of software used for design and verification, individuals accessing the design during the flow, etc. The data collection, independent assessment, and government provided information will inform the development of draft design standards for confidentiality and integrity.

Phase 2 from Task 3 will be a demonstration of implementation of those prototype standards

from Task 3 in at least one dual-use integrated circuit. Demonstration of implementation of those prototype standards from Task 3 in at least one custom DoD integrated circuit.

The table below reflects the number of total designs per year to support this prototype project.

Category	IOC	FOC	Scale
Capacity: Volume	**10/year**	**20/year**	**30/year**
Digital	**Required**	**Required**	**Required**
Mixed Signal	**Required**	**Required**	**Required**
Rad-Hard	**Not Required**	**Not Required**	**Not Required**
RF	**Not Required**	**Not Required**	**Not Required**
Security	ITAR	ITAR	ITAR/Classified

1.8. Rationale for Using an OT & Consistency with 10 U.S.C. 2371b

1.8.1. The subject project--

☒ Is *or* ☐ Is not directly relevant to enhancing the mission effectiveness of military personnel and the supporting platforms, systems, components, or materials proposed to be acquired or developed by the Department of Defense, or to improvement of platforms, systems, components, or materials in use by the armed forces.

Note: If the project is not directly relevant, please contact the S²MARTS Agreements Officer regarding project eligibility.

1.8.2. The effort can be characterized as a/an— (select all that apply)

☐ Proof of concept
☐ Model
☐ Pilot
☐ Reverse engineering effort to address obsolescence
☐ Novel application of commercial technologies for defense purposes
☐ Agile development activity
☐ Creation
☒ Design
☒ New Development
☐ Process
☐ Demonstration of technical or operational utility

1.8.3. The goal of the project is to result in a--

☒ Physical or virtual model(s), item(s), or report(s)
☐ Concept
☐ Other:

1.9 Strategic and Spectrum Missions Advanced Resilient Trusted Systems (S^2MARTS) Scope Determination

☒ STRATEGIC MISSIONS provide credible military options to deter aggression or coercion by adversaries that threaten vital interests of the United States or its allies. Strategic Missions efforts include nuclear weapons and their delivery platforms, conventional weapons that provide a similar global strike capability, missile defense systems and associated command, control and communications systems such as early warning radar and satellites, communication systems and electronic warfare systems. Endeavors in this arena provide full spectrum life cycle scientific, engineering and management functions to design, develop, test, evaluate, and acquire safe, reliable, secure and effective hardware for Strategic Systems which includes navigation, launcher, guidance, fire control and reentry systems. Tasking also includes advanced microelectronics to provide safe, trusted, reliable and effective advanced products. Associated areas of interest include counterfeit technologies, radiation-hardening, microelectronic devices, circuit cards, interconnect technologies, microelectronic controls, solid state transmit/receive modules, and other radio frequency devices. Microelectronics refer to electronic designs that are typically in the micrometer-scale or smaller.

☐ SPECTRUM MISSIONS include a wide variety of engineering, logistics and maintenance support for complex Electronic and Infrared Warfare systems and Platform Defense Systems to include maritime electronic warfare (EW), radar technologies, expeditionary EW, Infrared/Radio Frequency (IR/RF) systems technologies and airborne electronic attack systems.

1.9.1 Applicable Technology Areas Supporting Use of S^2MARTS *(check all that apply)*

☒ 1 - Verification & Validation
☐ 2 - Machine Learning
☐ 3 - Multispectral Sensing
☒ 4 - Design Assurance
☐ 5 - Field Programmable Gate Arrays
☐ 6 - Enhanced Fabrication
☐ 7 - Radiation Hardened Microelectronics
☐ 8 - Outreach and Standards
☐ 9 - Magnetic Random Access Memory
☐ 10 - Materials and Processes
☐ 11 - Manufacturing Technology
☐ 12 - Modeling & Simulation
☐ 13 - Radio Frequency (RF) and Optoelectronic Microelectronics
☐ 14 - New Microelectronics Development, Demonstration, and Capability Insertion
☒ 15 - COTS Programmable Integrated Circuit
☐ 16 – Microelectronics Obsolescence and Replacement
☐ 17 - Radiation Hardened by Process Radiation Hardened by Design
☐ 18 - Microelectronics and Electronic Warfare Focused Workforce Development
☐ 19 - Strategic Missions Hardware
☐ 20 - Spectrum Warfare Technologies related to cognitive/adaptive, distributed/ networked multispectral sensors, high power RF, spectral

agility, low probability of intercept communications, RF and infrared countermeasures, and coherent RF transmission

☐ 21 - Spectrum Warfare Technologies related to advanced and custom optics, advanced threat assessment and exploitation efforts

☐ Other – Provide a brief description of a related project not covered by Objective Areas 1-21 for consideration and approval:

Helpful Resources:

1. 10 U.S.C. Code § 2371b – Authority of the Department of Defense to carry out certain prototype projects: https://www.govinfo.gov/content/pkg/USCODE-2015-title10/pdf/USCODE-2015-title10-subtitleA-partIV-chap139-sec2371b.pdf

2. S2MARTS Technology Objective Areas: https://s2marts.org/technology-focus-areas/

3. NSWC Crane Prototype Project Process Flowcharts: *Embedded PDF below*

4. RAMP FLOW: Embedded PDF below

NSWC Crane_OTA Workflows.pdf

Approval Page Authorizing Pursuit of Project

Prepared/Submitted By:

Requiring Technical Authority

Title: Mr. Karl Franklin

Organization: NSWC Crane

Concurrence:

Requiring Activity Division Manager

Title: Mr. Brian Stuffle

Organization: NSWC Crane

Requiring Activity Deputy Dept. Head

Title: Mr. James R Ross

Organization: NSWC Crane

S2MARTS Program Manager

Title: Mr. Allen Tillerson

Organization: NSWC Crane

Office of Counsel

Title: Mr. Eric Vanwiltenburg

Organization: NSWC Crane

Approval:

Cognizant 02 Division Approval or Concurrence:

Title: Mr. Jordan Schnarr

Organization: NSWC Crane

NOTE: If Deputy Technical Director (DTD) is not required, the 02 Division is the final approver. If DTD approval is required, the 02 Division is providing concurrence.

Deputy Technical Director Approval (if required):

Title:

Organization:

NOTE: DTD Approval ONLY required if any reviewer of the information contained herein makes a determination that elevation to DTD is necessary. Examples for the elevating approval levels include but are not limited to 1) A prospective project with an External Requirements Owner; or 2) the prospective project is not clearly within Scope/Technology Areas (Enclosure 1).

PAA PART 2

Part 2 delineates key items that must be considered and documented prior to requesting approval for release of a Request for Solutions.

2.1 Project Management Structure:

This project will be managed and monitored by a technical team consisting of engineers, technicians, scientists, acquisition professionals from NSWC Crane and/or other subject matter experts (SMEs) in the DOD.

A member or members of the Government team will be designated as an Agreements Officer Representative (AOR) depending on the final number of selected solutions. The AOR is responsible for monitoring performance – to include tracking all deliverables.

The project management team will determine technical entrance and exit criteria to each task and stage of this project, as well as validate success in meeting the requirements of this project, once Request for Solution (RFS) responses are received and specific solution capabilities are known.

Position/Title	Name/Organization
S^2MARTS Program Manager	Allen Tillerson
Prototype Project Selection Official	James R Ross
Agreements Officer	Dallas Parsley
Agreements Specialist	Mary Beth McFann
Requiring Technical Authority	Karl Franklin
RA Deputy Department Head	James R Ross
Agreements Officer Representative	Bryan Smith

2.2 Project Deliverables (and location of physical deliveries, if applicable):

Item No.	Item/Deliverable	Quantity/ Frequency	Deliverables
1	Phase 1 Draft RAMP Report comprised of the following elements: • Task 1 Detailed description of the Secure Design Capability • Task 2 Methods to Ensure Confidentiality and Integrity of ICs/SoCs • Task 3 DoD Supply Chain Security standards along with justification for those standards	1/Once	No Later Than four (4) months from project award.
2	Phase 1 Final RAMP Report comprised of the following elements: • Task 1 Detailed description of the Secure Design Capability • Task 2 Methods to Ensure Confidentiality and Integrity of ICs/SoCs • Task 3 DoD Supply Chain Security standards along with justification for those standards	1/Once	No Later Than six (6) months from project award.
3	Phase 1 Technical Interchange Meeting (TIM) and Meeting Minutes	6/Monthly	Five (5) business days after previous month's end
4	Phase 2 Design Review	4/Quarterly	Five (5) business days after previous Quarter end
5	Phase 2 RAMP Demonstration of the following elements: • Task 1 Secure Design Demonstration • Task 2 Design Demonstration on the below: o SOC o Digital IC o Mixed-signal IC • Task 3 Supply Chain Demonstration on the below:	1/Once	No later than eighteen (18) months from Phase 2 award

	o Dual-use IC o Custom DoD IC		

2.3 Security Classification, Respondent Restrictions, and other Required Compliance

a. Security Classification:

Unclassified

b. Is ITAR Compliance required?

Yes

c. Respondent Restrictions (e.g., domestic companies only):

N/A

d. Hazardous Material:

N/A

e. Any additional restrictions applicable to this project:

2.4 Market Intelligence

a. Recommended North American Industrial Classification System (NAICS) for publicizing purposes:

541713

b. Recommended Product Service Code (PSC)/Object Class Code (OCC) for publicizing purposes:

PSC AD93 OCC 255

c. Market Trends

☐ New/Emerging Technology Market

☒ Established Commercial Market

☐ Current market includes legacy providers who cannot meet technical objectives

d. Potential Solution Providers

☐ Market conditions & potential providers for this technology are unknown

☒ A summary of known potential providers related to this technical area include:

Organization	Member/Non-member	Capability
Analog Devices	Non-member	Commercial IC designer and IC provider.
Ansys	Non-member	System-/high-level electronic design and simulation provider; workflow provider
Arm	Non-member	Third-party microelectronics intellectual properties provider.
Avago Technologies	Non-member	Commercial IC designer and IC provider.
BAE Systems	Member	DoD IC Design and prototype Experience (including ITAR); Non silicon process (e.g. GaN)
Boeing	Member	DoD IC Design and prototype Experience (including ITAR)
Broadcom Inc.	Non-member	Commercial IC designer and IC provider.
Cadence	Non-member	Third-party microelectronics IP provider; Advanced node electronic design automation provider; hardware emulation; Reference ASIC and IP workflows
Edaptive Computing, Inc.	Member	Workflow Development
Facebook	Non-member	Big Data and AI
GlobalFoundries	Non-member	Advanced Node Silicon Processes and reference ASIC and IP workflows
Google	Non-member	Big Data and AI
I3electronics	Non-member	Advanced packaging and printed circuit board manufacturer and assembler
IBM	Member	Big Data and AI; foundry and IC experience
Intel	Member	FPGA silicon design, microprocessor designs, Advanced node silicon processes
Keysight	Member	Advanced HW testing equipment manufacturer; electronic design automation provider; Possible RF and system modeling workflows

Organization	Member/Non-member	Capability
Maxim Integrated	Non-member	Commercial IC designer and IC provider.
Mentor (a Siemen's Company)	Non-member	Advanced node electronic design automation provider; hardware emulation; ASIC and IP workflows
Micron	Non-member	Commercial IC designer and IC provider.
Nimbis Services	Non-member	Cloud-based microelectronics design environment with hook-ins for virtual testing laboratories, provenance, traceability, and IP management supportive of advance EDA tools
Northrop Grumman	Member	DoD IC Design and prototype Experience (including ITAR)
Qualcomm	Non-member	Design and AI, Telecommunications 5G; Commercial IC designer and IC provider.
Raytheon	Member	DoD IC Design and prototype Experience (including ITAR)
Samsung	Non-member	Advanced Node Silicon Processes, Big Data, and AI
Synopsys	Non-member	Third-party microelectronics IP provider; Advanced node electronic design automation provider; hardware emulation; Reference ASIC and IP workflows
Tesla	Non-member	Big Data and AI; automotive
Texas Instruments	Non-member	Commercial IC designer and IC provider.
Tortuga Logic	Non-member	electronic security design automation provider
Xilinx	Member	FPGA silicon design

☒ The list includes nontraditional defense contractors (to include small businesses)

☐ The list includes traditional defense contractors only.

If any of the above potential solution providers have worked on previous similar efforts please identify the company, the contract number, and a brief description of the effort performed below, or select Not Applicable ☐

Company Name	Contract No.	Description
N/A	N/A	N/A

2.5 Significant Risks & Mitigations (if applicable):

a. Technical -

Concern(s): The technical risk is minimal as most of the technical capabilities individually exist in the commercial sector.

Mitigation(s): The evaluation team will be comprised of experts who will be prepared to evaluate the technical expertise and demonstrated capabilities of each respondent.

b. Price / Affordability -

Concern(s): The cost risk will be evaluated at the end of Phase I upon receipt of the detailed technical and business plan and must be sufficiently addressed to progress to the optional Phases.

Mitigation(s): Each phase will be evaluated for fair & reasonable pricing, as well as overall affordability, prior to execution of each new phase.

c. Schedule -

Concern(s): Schedule is of the greatest concern given the criticality of this technology for DoD weapon system modernization.

Mitigation(s): Phase I will deliver a schedule, based in demonstrated capabilities and expertise. It will be incumbent on the Government project management team to continuously monitor status and ensure that milestones are met, and if not work with the performer on mitigation plan for getting back on schedule.

2.6 Project Duration

The project's period of performance will be defined based on the performer's proposed schedule, but is estimated to be complete within 24 months for the entire effort.

The Government anticipates that a follow-on production contract or transaction may be awarded to the performers for this effort without the use of competitive procedures if the participants in this transaction successfully complete the prototype project as outlined within their transaction. The follow-on production effort would involve the potential requirement for additional technology refinement or integration into existing programs of records or the future Strategic or Trusted Microelectronics programs.

2.7 Evaluation and Selection Strategy

Selection Process:

Please select how you would like to initially review and assess the respondents' ability to meet the project's technical objectives:

Technical Submission:	Price Submission:
Written Proposal	Standard Price Proposal

Will the project benefit from a multi-stage evaluation approach? If so, please select how the subsequent engagement will be conducted. If not, please proceed to the Proposed Solution Assessment Team table and populate the requested information:

Follow-On Technical Assessment:	Price Assessment:
Choose an item.	Choose an item.

Proposed Solution Assessment Team

Name	Position/Title	Organization	Govt. or KTR
Karl Franklin	Engineer	NSWC Crane	Govt
Matt Sale	Engineer	NSWC Crane	Govt
Len Orlando	Manager	Air Force Research Lab	Govt
Brett Hamilton	SSTM	NSWC Crane	Govt
TBD	TBD	NSA	Govt