S²MARTS Project 20-06: Rapid Assured Microelectronics (RAMP)

Request for Solutions (RFS) Questions & Answers | Posted April 27, 2020

1. **Question**: What are the threshold and objective instantaneous bandwidths?

   Response: We assume this question relates to potential RF applications. This is technology and application dependent. The primary objective of RAMP is the ability to perform the physical design of ICs utilizing technologies available from 22nm and below foundries. We are not focused on a particular application or requirement at this time.

2. **Question**: What are the threshold and objective update rates?

   Response: The primary objective of RAMP is the ability to perform the physical design of ICs utilizing technologies available from 22nm and below foundries. We are not focused on a particular application or requirement at this time.

3. **Question**: What is the desired field or area of regard?

   Response: Any DoD application that warrants SOTA ≤ 22nm technology.

4. **Question**: What is the target application? Maritime, Bluewater, Littoral or Expeditionary use?

   Response: Any DoD application that warrants ≤ 22nm technology, including, ground, aircraft, space, and the above mentioned Navy systems.

5. **Question 5**: Is the baseline GFE or performer discovered?

   Response: The government will not be providing baseline GFE in order to perform.

6. **Question**: Is the intent of the program to create a secure design capability that can utilize foreign foundries (like TSMC) and potential use of foreign layout? but... - cannot be corrupted or discovered during the layout process - ensure a secure backend flow such that design is not \"known\" and cannot be corrupted during manufacturing or is the intent to move these functions on-shore as much as possible to US based foundry like Global Foundries and US resources?

   Response: The intent of the program is for the DoD to be able to access commercial SOTA semiconductor fabrication processes, while ensuring the confidentiality and integrity of the circuit design, and mitigating the need for International Traffic in Arms Regulations (ITAR) fabrication. This is true for both on-shore and off-shore foundries. This RFS is targeting foundry independent, secure, on-shore, physical or back-end design capability that can support SOTA ≤ 22nm fabrication technology.

While on-shore foundries are preferred, off-shore foundries could be considered given sufficient justification and ability to demonstrate quantifiable assurance.

7. **Question**: Is the intent to use US foundries only? Is the intent of the program to enable offshore foundries?

   Response: The intent of the program is for the DoD to be able to access commercial State-of-the-Art (SOTA) semiconductor fabrication processes, while ensuring the confidentiality and integrity of the circuit design, and mitigating the need for International Traffic in Arms Regulations (ITAR) fabrication. This is true for both on-shore and off-shore foundries. This RFS is targeting foundry independent, secure, on-shore, physical or back-end design capability that can support SOTA ≤ 22nm fabrication technology. While on-shore foundries are preferred, off-shore foundries could be considered given sufficient justification and ability to demonstrate quantifiable assurance.

8. **Question**: Does one shore fabrication add value?

   Response: While on-shore foundries are preferred, off-shore foundries could be considered given sufficient justification and ability to demonstrate quantifiable assurance.

9. **Question**: Is there expectation to modify standard foundry offerings to ensure security, integrity and confidentiality during the manufacturing flow?

   Response: No process modifications are expected to the standard foundry offerings. This is outside the scope of this RFS. The foundry should be treated as a black-box as much as possible to manage the scope.

10. **Question**: This task will define ways to leverage commercial supply chain security methods to meet DoD needs and are compatible with commercial manufacturing practices. 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. Does this Task imply that fabless semiconductor developer in the DIB will have access to foundry-related data, for example to enable yield and failure analysis? For Task 3, can we assume that ASIC foundries will provide relevant data, for example wafer images or process-specific data? Are there specific chain-of-custody methods assumed or prohibited in the RFS, for example use of Blockchain technologies?

    Response:
    a. The Government cannot provide access to foundry-related data. The performers will have to negotiate that access if required for their proposed solution.
    b. Leveraging and adding to existing best practices, which are heavily driven by yield and reliability is of great interest for enabling quantifiable assurance.
    c. No specific chain of custody methods are assumed or prohibited.

11. **Question**: RFS-Attach-1_Rapid-Assured-Microelectronics-RAMP-Flow.pdf. The graphic placement seems to imply that Confidentiality applies to RAMP and Integrity applies to SHIP. Is that the intention? Does the government consider a design center capability to be a design center, or service, or a flow that any DIB designer can use?

    Response: That was not the intention. Both Confidentiality and Integrity applies to the entire manufacturing/fabrication process, which includes the capability that RAMP is addressing. .

12. **Question**: 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 Do DIB entities and IP partners need to be entirely US-based, or is the Solution intended to secure and optimize design and verification that includes non-US organizations, for example a processor IP vendor? Does Task 1 include creating secure environments for non-US collaboration, for example collaborating with an offshore Design Services partner? Does Task 1 include the entire RTL (or mixed-signal) RTL to GDSII flow including back-end physical verification including RTL and mixed-signal simulation, physical synthesis, Static Timing Analysis, Power Analysis, Design Rule Check? Is hardware emulation in scope for Task 1? Are providers of software solutions (EDA, Yield Analysis, Design/IP management or otherwise) required to be U.S. based firms?

    Response:

    a. There are no constraints on IP vendors, however the core execution team must adhere to DoDI 8582.01
    b. It covers the entire flow, which is needed ensure a working design
    c. Hardware emulation is not required, but would needed by programs to simulate large ASIC designs
    d. See Question 71

13. **Question**: 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. Does Task 1 include applications related to lithography/OPC? Are manufacturing-related workflows, for example yield analysis, in scope for Task 1? What levels of DoD compliance are required or desirable, beyond ITAR?

    Response:

    a. The goal is for the team to be experienced with the PDK and prior tape-outs in that process node and foundry such that they would have insight into the more subtle issues of the PDK and manufacturing related workflows.
    b. Yes
    c. Respondents must comply with documentation identified in the RFS like DoDI 8582.01 and DoDM 5200.01 Volume 4 and other documents specified.

14. **Question**: 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. Does this include monitoring and analyzing data from the foundry/manufacturing process, for example using data generated during Etch, Deposition, etc.?

Response: If such data contributes to the proposed quantifiable assurance solutions.

15. **Question**: What are the \"obsolete practices\" used for backend design? Is there something specifically targeted to be replaced/updated?

    Response: Nothing is specifically targeted to be replaced from the standpoint of tools or methodology. The intent is to move from small and fragmented in-house back-end design teams that complete very few projects per year to an external vendor. The assumption is that the chosen vendor will already have experience in this type of business model. The desire is to put in place an arrangement with a small subset of potential vendors to perform the majority of the physical design of ASICs and SoCs for DoD applications, including supporting the needs of the defense industry

16. **Question**: What does \"confidentiality of circuits\" during manufacturing mean?

    Response: Per the RFS Attachment 1 flow graphic: "*the protection of sensitive design information during the implementation and manufacturing process*."

17. **Question**: How are confidentiality and integrity defined? - How are confidentiality and integrity going to be measured?

    Response: Confidentiality and integrity are defined on RFS-Attach-1_Rapid-Assured-Microelectronics-RAMP-Flow.pdf. There is no specific criteria on how they will measured, they will be evaluated by Government assessment team.

18. **Question**: Integrity is defined as alterations of the design during the manufacturing. Does this mean tampering with design shapes such as adding/deleting shapes in manufacturing, or tampering with the fabrication process such as etch recipe?

    Response: Integrity is concerned with any unanticipated or un-attributable alterations.

19. **Question**: Section 5, Phase 1 objectives, Task 2, page 4: The definition of Integrity refers to the manufacturing process. Does the Integrity threat model addressed by RAMP include the design phase as well as fabrication phase?

    Response: The Integrity threat model addressed by RAMP is focused on the physical design process that refers to the post Register Transfer Level (RTL) portion of design that includes automated place and route, timing closure, and verification of the physical design.

20. **Question**: 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. Does Task 2 include IP validation (equivalence checking) post-fabrication, for example to detect unauthorized IP insertion? Is wafer inspection considered to be part of Task 2?

Response:

a. IP validation (equivalence checking) would help ensure no unanticipated or un-attributable alterations of the design during the manufacturing process.
b. Wafer inspection directly is not part of this task, while any technique implementable during the RAMP related design process that enables or enhances the ability to do wafer inspection is in scope.

21. **Question**: Is the intent of the supply chain security, integrity and confidentiality processes for RAMP meant to cover through Wafer fabrication only or through packaging and test?

Response: The intent is to cover IC and SoC design/fabrication supply chain. SHIP will cover packaging and testing.

22. **Question**: Will DoD provide the government sponsored best known Confidentiality & Integrity methods and in what form and timeline?

Response: The intent is respondents will provide the recommended Confidentiality and Integrity methods leveraging existing commercial best practices to the greatest extent possible.

23. **Question**: What is the threat model we're working to protect against?

Response: Any threat in the physical design process that would affect the intended functionality, performance or reliability of an ASIC or IC design.

24. **Question**: - Who is responsible for certification of ITAR/non-ITAR and Classified/Un-Classified and transition from one to the other and back? - What existing government standards/requirements like ITAR will be applied? When? The ITAR guidance as stated to \"mitigate the need for ITAR fabrication\" then on page 8 it states ITAR compliance is required.

Response: There are several questions posed above.

Who is responsible for certification of ITAR/non-ITAR and Classified/Un-Classified and transition from one to the other and back?

1. The classification of this program is Unclassified. Although classified items (articles, technical data and defense services are on the USML (Category XVII)) fall under ITAR. Classified items are outside the scope of this RFS.
2. The Directorate of Defense Trade Controls (DDTC), **U.S. Department of State**, administers the International Traffic in Arms Regulations (ITAR) (22 CFR parts 120 through 130). ITAR is a self-certification compliance program.

- International Traffic in Arms Regulations (ITAR) control the export and import of defense-related articles and services on the United States Munitions List (USML). All manufacturers, exporters, and brokers of defense articles, defense services, or related technical data must be ITAR.

- Companies engaged in the manufacturing, exporting, temporary importing, or brokering of defense articles (including technical data), or provisioning of defense services controlled by ITAR (see the U.S. Munition List (USML)) must be "ITAR certified (compliant)". ITAR compliant includes the following (1) Registration with the DDTC, (2) maintenance of records required by 22 CFR §122.5 , and (3) obtaining licenses or other approvals prior to making exports, temporary imports, or engaging in brokering activities

3. A government team of SME will assess the proposed solutions and determine if the tools and methods developed under this RFS will mitigate the need for ITAR fabrication. The DoD will work closely with the State Department to ensure compliance with ITAR regulations.

What existing government standards/requirements like ITAR will be applied? When?

4. See question 25 regarding clarification DDTC has published regarding ASICs and programmable devices. In addition, the DoD is actively working on updating related policies (e.g. DODI 5200.44) and corresponding guidance to the community

The ITAR guidance as stated to \"mitigate the need for ITAR fabrication\" then on page 8 it states ITAR compliance is required

5. The RFS is soliciting proposals to develop novel and innovative methods including unique and secure design tools and critical circuit modules required to design advanced custom ICs and SoCs. By definition, the Respondents working on the development of these tools and circuits must be ITAR compliant. These tools will allow the DoD to mitigate the need to manufacture the integrated circuits in an ITAR compliant foundry. In summary, the Respondents to this RFS must be ITAR compliant, the foundries do not need to be ITAR compliant.

25. **Question**: We understand that the government (DoD & DoC) is working on new rules on ITAR for electronics "relaxing some of the existing requirements. Can you provide a reference to the latest ITAR requirements?

Response: Department of Defense worked with Department of State and achieved consensus that if USML capability is not present at manufacturing (hard-wired) then the device is treated as a programmable device and is not controlled until it is programmed for a defense article (post manufacturing).
To that end, Department of State has published a clarification in the ITAR FAQ section.

ITAR / USML Updates FAQs:
Q: We manufacture integrated circuits (ICs) that are unique for defense articles and include programmable elements. Are these ICs described by USML Category XI(c)(1)? How does Note 3 to USML Category XI(c)(1) apply when the programmable elements are un-programmed?

A: An IC that is unique to a defense article is described in USML Category XI(c)(1). An IC that contains both programmable elements and non-programmable elements may only be treated as a Programmable Logic Device (PLD) when all of the non-programmable elements are common to an IC used in an item that is not a defense article. When these conditions are met, Note 3 to USML Category XI(c)(1) applies, and the IC is not controlled by USML Category XI(c)(1) so long as all of the programmable elements are un-programmed.

The non-programmable elements referenced above are the larger cores, blocks of logic, or functionality developed for reuse in different IC designs, and not the discrete IC elements such as transistors, diodes, resistors, capacitors, or conductive pathways that are constituents of the non-programmable elements.

If doubt remains as to whether an IC is a USML Category XI(c)(1) article, a Commodity Jurisdiction Determination request may be submitted to the State Department via the DDTC website. Submissions should clearly identify the major cores or blocks of logic, their origin, their function(s), and the types of interactions with the other cores or blocks on the IC.

The link is:
https://www.pmddtc.state.gov/ddtc_public?id=ddtc_public_portal_faq_detail&sys_id=8215c8a9db9bb3807ede365e7c9619d5

26. Question: (Multiple Questions) RFS Section 8.b " Security Classification Compliance on page 7. This section states that ITAR Compliance is required.

a. Please confirm that the question is actually inquiring as to whether the respondent is registered as a manufacturer with the Directorate of Defense Trade Controls (DDTC).
b. Are subcontractors required to be registered for ITAR purposes with (DTTC) if its performance will not involve the use of any ITAR requirements?
c. Can a subcontractor use non-USNs for performance if their work is classified for this requirement?
d. Could the Government confirm that the FOCI documentation and mitigation plan requirements only applies to foreign owned subcontractors that are pursing classified work on this program?

Response:
a. Yes, Respondents must be compliant with ITAR regulations and be registered with the State Department's Directorate of Defense Trade Controls (DDTC).
b. Respondents to this RFS are restricted to domestic companies only and respondents performing work shall as a minimum be U.S. Citizens. Subcontractors supporting the primary performer can be foreign owned firms, but that relationship must be completely firewalled from any ITAR or CUI related information.
c. Respondents to this RFS are restricted to domestic companies only and respondents performing work shall as a minimum be U.S. Citizens.
d. FOCI requirements only apply to those who are Foreign Owned Controlled or Influenced. Otherwise, a mitigation plan is not required.

27. Question: Government Purpose Rights section may require changes post phase 1, will the government revisit this section and its intent post award. - Based on GFI/GFP; are designs categorized as such

Response: Any alterations or modifications to the resultant Performer's Agreement (which is the contract that codifies the project) will be implemented as bilaterally determined by the Performer and Government, and directed by the Government to NSTXL.

28. **Question**: Are there specific IP and or capabilities that are targeted in the <22nm (FinFet) process nodes desired as part of the program?

    Response: In general, typical SoC IP including but not limited to: a variety of processor cores, multicore, NOC, non-volatile memory, single and multiport SRAM, PLLs, ADCs, DACs, DSP, ML, AI, Ethernet, USB 2 and/or 3, etc.

29. **Question**: Has the challenge outlined in RAMP already been addressed for all process technologies, with geometries greater than 22nm

    Response: No, there has not been a RAMP process for nodes greater than 22nm.

30. **Question**: Is there an intent to leverage the Chiplet technology concepts used in large SOTA commercial SOCs as an output of this program

    Response: This should support both Chiplet, SoC, and conventional ASIC end products. The packaging type or style is outside the scope of this project. Page 2, paragraph 3: "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."

31. **Question**: Are foreign companies allowed to participate or be leveraged? i.e. largest fab with <22nm is TSMC Assuming this is true if target is assured flow through non-US foundries and / or use of international backend resources

    Response: Respondents to this RFS are restricted to domestic companies only and respondents performing work shall as a minimum be U.S. Citizens. While on-shore foundries are preferred, off-shore foundries could be considered given sufficient justification and ability to demonstrate quantifiable assurance.

32. **Question**: RFS Section 8.a - Security Classification Compliance on page 7. Please advise if respondents should expect Covered Defense Information to be provided to the contractor by or on behalf of Government in support of the performance of the OTA, or Covered Defense Information to be collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the OTA?

    Response: The Security classification for this program is Unclassified. Controlled Unclassified Information (CUI) is an umbrella term that encompasses all Covered Defense Information (CDI) and Controlled Technical Information (CTI). As stated in Section 8.a.:

    - Respondents must be compliant with DoDI 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems" and DoDM 5200.01 Volume 4, "DoD Information Security Program: Controlled Unclassified Information."

    - Respondents must implement the security requirements in NIST SP 800-171, "Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations."

Respondents are expected to receive, generate, and handle CUI in accordance with DoDI 8582.01, DoDM 5200.01, and NIST SP 800-171. CDI includes:

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract
(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

33. **Question**: RFS Section 8.a - Security Classification Compliance on page 7. Please confirm the requirement for Respondents performing work shall as a minimum be U.S. Citizens. This seems inconsistent with the request for a solution using commercial best practices. Do all performers need to be US Citizens? Permanent residents OK? if US Citizenship required for IOC/FOC, can this requirement be relaxed for Phase 1?

Response:

a. As stated in Section 8.a, Respondents performing work shall as a minimum be U.S. Citizens. This requirement is for the respondents to this RFS who will be working on the development of novel and innovative methods including unique and secure design tools and critical circuit modules required to design advanced custom ICs and SoCs. This requirement does not apply to the commercial foundries. The solution proposed should "leverage" and be "compatible" with commercial best practices.
b. Yes
c. This requirement cannot be relaxed for Phase I.

34. **Question**: RFS Section 5 Phase 1, Task 1 Secure Design Capability, page 3: not tied to a single fabrication facility / flow: Does this mean different companies/ entities entirely, or can it be different process nodes at different sites within a single company, or a single process node at 2 different sites within the same company?

Response: Any or all of the above. The DoD is looking toward utilizing assurance technologies with the greatest flexibility for access to SOTA semiconductor manufacturing processes. The respondents should address the technical feasibility and limitations of the proposed solutions (i.e. compatibility with different foundries, technology nodes, and/or process flows)

35. **Question**: Section 5, Desired End-State Objective(s) & Success Criteria, page 2: Please provide details on Phase 3 (Validation of Designs Using the IC and SoC Physical Design Infrastructure).

Response: There will be no Phase III and it will be removed from the RFS.

36. **Question**: The below questions pertain to the DoD relevant designs described in Section 5, Phase 2 Objectives on page 5 of the RFS. a) What is the expected die area (area range is OK) for the 3 Prototypes? b) What are the initial prototype volume requirements? Are additional volumes required post prototype delivery? c) What are the commercial application specific IPs required for the Prototypes? d) Will each prototype development require multiple development methodologies? i.e., PD support only, turnkey PD, etc. a. For turnkey PD: What is the deliverable? Full timing converged netlist?

b. What is the test coverage implementation and who is the test implementation owner? Will functional test vectors be provided? e) What is the evaluation criteria for the Prototype? Power, Performance, Area?

Response:

a. Area: not pre-defined, will be driven by application, could range from a small chiplet to a large SoC
b. Prototype Design minimum Volume targets: per table 2, Capacity: Volume 5/year (IOC), 10/year (FOC-driven by demand)
c. IP: TBD, likely as wide-ranging as possible: "the SoC proto-type design demonstrator will incorporate commercial and DoD application specific IP, the Digital IC and mixed-signal IC will as well"
d. Methodologies: no
    - Turn-key Physical Design: Admittedly somewhat confusing wording. This should assume that functionally verified RTL is delivered and that the physical design team performs all steps from RTL synthesis through "tape-out" including test insertion and ATPG.
    - Test coverage implementation and owner: Depends on the chosen flow. Multiple options are desired.
e. While PPA are important and cannot be ignored, turn-around-time and cost are at least as important if not more so. The physical design process must be rapid, assured and efficient (to drive down schedule and technical risk, as well as cost).

37. Question: As the intent is for the IP to have government use rights at 5 yrs and beyond ; for the Phase 2 Commercial and Application specific IP, and Digital IC implementation designs is there a class of performance minimum that should be assumed for , standard interface, Memory and/or storage interface IPs that could be used in these designs ?

Response: No minimum performance is specified. The designs selected will be DoD relevant, which will drive the expected performance.

38. Question: (Multiple) Please clarify that that the total project budget of $50M is intended to be partitioned amongst multiple awardees. As opposed to multiple $50M awards.

Response: The total project budget of $50M is intended to be partitioned amongst multiple awardees.

39. Question: Attachment 1 depicts a flow/activity diagram correlated to the SHIP program. No such narrative description is presented to detail the extent of interoperability of data/information in the RFS. Was this intentional and left up to proposers to interpret the relationship?

Response: Attachment 1 was intended to show where RAMP fits in the overall design flow.

40. Question: What is the definition of a dual-use IC?

Response: Dual Use" is defined in Section 772.1 of the EAR as: Items that have both commercial and military or proliferation applications. While this term is used informally to describe items that are subject to the EAR, purely commercial items are also subject to the EAR (see §734.2(a) of the EAR).

See also 78 Fed.Reg. 22660 (April 16, 2013) at page 22688 which notes: Central to the existing ITAR and EAR export control structures is the concept that an item is not ‘‘specially designed’’ for a controlled item if it was deliberately made for use in both controlled and uncontrolled applications, i.e., a ‘‘dual-use’’ item

41. **Question**: How does the government define correlation? Is this a capability that the RAMP solution should provide or is this sentence only intended as background information?

    Response: In section 4 of the RFS, “is developing integrated circuit (IC) hardware and workflow prototypes that promote the use of assurance principles, feature protections, and correlation.” - in this case, is the process of establishing a relationship or connection between two or more measurements of related quantitative data. For example, between design steps or manufacturing steps.

42. **Question**: What DoD application specific IP will be used? Will any DoD IP require additional development on the RAMP program and what level of complexity?

    Response: IP requirements will be based on the proto-type design application demonstrators selected. It is not the intent of RAMP to develop design IP.

43. **Question**: Will the DoD provide the performers with designs for Phase 2 and 3 or are the performers to provide designs? If the DoD is providing designs for Phase 2 and 3, how should performers price that effort?

    Response: The DoD will not provide the performers with designs for Phase 2. All demonstration designs will be selected in coordination with the DoD evaluation team. No Phase 3 is planned and the RFS will be updated to remove.

44. **Question**: Is the Phase 2 Task 3 Demonstration IC different from the Task 2 designs and is this to also be completed within the 18-month period of performance?

    Response: These include demonstration of the flow/process, as applied to demonstration proto-type designs. All Phase 2 work should be completed in 18-month period of performance.
    Phase 2 RAMP Demonstration of the following
    elements:

    • Task 1 Secure Design Demonstration

    • Task 2 Design Demonstration on the below:
    - SOC
    - Digital IC
    - Mixed-signal IC

    • Task 3 Supply Chain Demonstration on the below:
    - Dual-use IC
    - Custom DoD IC

45. **Question**: Phase 2 describes the design & fabrication of at least Three DoD Relevant designs: (1) SOC, (2) Digital IC, (3) Mixed Signal IC. However, Task 3 of Phase 2 describes the demonstration of implementation of prototype standards From Task 3 in at least one Dual Use IC and at least one Custom DoD IC. The second reference to Task 3 is believed to reference to Task 3 of Phase 1 which is, Definition of DoD supply chain standard that leverages commercial microelectronics supply chain security methods to meet DoD needs What is the relationship between the Dual Use & Custom ICs and the Three DoD Relevant designs, if any? Are the Custom DoD IC and the Dual Use IC separate and additional designs, as compared to the Three DoD Relevant designs? Do the Custom DoD IC and Dual Use ICs of Task 3/Phase 2 require separate and additional fabrication, in addition to the fabrication of the Three DoD Relevant designs?

    Response: Task 3 is "Supply Chain Demonstration", thus the intend is to address assurance of the supply chain required to design of Task 2 demonstration designs. This should develop standards, processes and best practices to elevate assurance in implementing the proto-type design flow. The Custom DoD IC and Dual ICs are included as the sources and nature of those supply chains and the availability of quantitative data could differ.

46. **Question**: RFS states: \"apply the best known methods, including government sponsored and commercially developed, for ensuring confidentiality and integrity of integrated circuits through the fabrication process\" and \"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\" If tools, processes, methods, need to be enhanced or gaps filled in this process, is this comprehended under RAMP?

    Response: RAMP expects the performer to identify all enhancements or gaps in the execution of a Secure Design Capability to enhance confidentiality/integrity assurance.

47. **Question**: 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 Does provenance and traceability include foundry-related process data, for example wafer images and recipes?

    Response: It does not include Foundry related process data, while any technique implementable during the RAMP related design process that enables or enhances the ability to leverage foundry-related process data could be of value to other T&AM execution areas whom are addressing post-foundry assurance methods.

48. **Question**: Task 3 from Phase 2 will be a demonstration of implementation of those prototype standards from Task 3 in at least one dual-use integrated circuit. Phase 2 does have Tasks, can you clarify Task 3 from Phase 2 in this text?

Response: (see question 44 and 45) In the Project Deliverables table, there are tasks identified under Phase 2 (item #5 in the table). Task 3 from Phase 2 will be a demonstration the implementation of the DoD supply chain security standards from Task 3 of Phase 1.

49. **Question**: RFS states: \"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.\" Do you expect that new supply chain security methods will also need to be developed as part of the RAMP initiative or should performers only focus on existing methods?

    Response: RAMP expects the performer to develop new methods if needed.

50. **Question**: What scoping information will be made available? When should performers plan to provide the costing associated with that work?

    Response: The "scoping information" is provided in the RFS. Respondents should provide their Statement of Work (SOW) for this effort and a cost proposal for Phase I with ROM estimates for following phases.

51. **Question**: How many reference designs will be identified & will they be executed in parallel? Will the reference designs be monolithic and/or heterogeneous?

    Response: Phase 2 requires to test at least three DoD relevant Designs. Some of the work will have to be in parallel to meet the 18-month timeline.

52. **Question**: RFS states: \"All demonstration designs will be selected in coordination with the DoD evaluation team.\" When will this occur? Who is responsible for the selection? What criteria will be used?

    Response: This will occur at the beginning of Phase 2. They will be selected in coordination with the government led evaluation team and will be based on DoD weapon system program needs.

53. **Question**: 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. Are these relevant designs required to be new, or can they be existing reference designs?

    Response: Designs should target DoD applications, ideally with identified transition paths to DoD programs. They will be selected in coordination with the government led evaluation team based in large part on the mission capability the design will enable.

54. **Question**: How does this solicitation align with the requirements, timelines, and budget priorities outlined in the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) Microelectronics Modernization Roadmap? What is the government's desired operating model post FOC?

Response: This aligns directly with the OUSD(R&E) roadmap for Microelectronics. The desire at FOC is that this investment will enable a self-sustainable commercially owned and operated capability.

55. Question: Section 6, Project deliverables, page 6: Deliverables include four quarterly design reviews in Phase 2. Does this imply that the chip design is expected to take 12 months, and then fabrication and test will be completed in the remaining 6 months?

Response: Yes, Chip design and fabrication is included in the 18 month schedule.

56. Question: Should Program Management be described and priced as a separate task, or should program management cost be distributed across each of the technical tasks?

Response: Program management should be broken out, especially if multiple performers are teaming for the proposal execution.

57. Question: Does the proposal require pricing for Phase 1, and then ROM cost estimates for Phases 2 and 3?

Response: Proposal is to provide technical/costs related to Phase 1 and estimates for Phase 2. There will be no Phase 3 and it will be removed from the RFS.

58. Question: Section 7, page 7 -You state that Multiple awards are anticipated. Will the government integrate the outputs of multiple awardees? Or, are competing parallel efforts expected? If the latter, how will the competing efforts be down-selected for possible follow on production effort? Since multiple awards are planned for Phase 1, will there be a consolidation to a single Phase 2 award?

Response: The Government anticipates multiple awards for Phase 1 and competing in parallel. Then a down select will happen before Phase 2 begins. The Government anticipates awarding one or 2 Phase 2 awards.

59. Question: Section 8, page 7 Can the government provide a draft DD254 in order to ascertain the clearances, DFARs and potential CMMC compliance? Will the Government please confirm and discuss when a Security Classification Guide will be made available?

Response: "Phase I awards will be unclassified and a DD254 will not be required. It is anticipated that a DD254 might be needed for future phases."

60. Question: Section 8, page 7 To what contractor IT systems does the Government intend for NIST 800-171 to apply? Is it just the design capability or will other IT systems be involved? If cloud services are used, what security requirements will apply? When is compliance with these standards desired, and will the Government consider waiver requests from individual controls?

Response: RAMP will require the performer to access Controlled Unclassified Information provided by the Government to complete the project and must follow government guidelines for protecting. Cloud

services if implemented would have to meet government guidelines as well. The government cannot waiver compliance for IT systems.

61. **Question**: Section 8 states that respondents must be compliant with: a. DoDI 8582.01, Security of Unclassified DoD Information on Non-DoD Information Systems, b. DoDM 5200.01 Volume 4, DoD Information Security Program: Controlled Unclassified Information, c. Security requirements from NIST SP 800-171, Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations, d. The National Industry Security Program Operating Manual (DODINST 5220.22M), and e. Any written instructions from the NSWC Crane Security Officer. Will the DoD be willing to work with commercial non-traditional government contractors to enable use of their current best practices rather than showing compliance to Govt specifications related to the handling of FOUO information that meet the intent of these requirements? Will there be any Controlled Unclassified Information provided by the Government to complete the project?

    Response: Document processes for compliance. NIST SP 800-171A provides a generalized framework for how the Government assesses compliance with NIST SP 800-171. There's also a System Security Plan Template, Plan of Action Template, and Mapping Cybersecurity Framework document on the NIST website that might help. RAMP will require the performer to access Controlled Unclassified Information provided by the Government to complete the project and must follow government guidelines for protecting.

62. **Question**: Section 9, paragraph 2, page 8 Need clarification of the intent of the second paragraph in Section 9. This appears to be a request for a copy of ALL work product from the project, not just the deliverables called out in Section 6. As this is a bit unusual, please confirm that this is indeed the intent of this.

    Response: The paragraph is correct, the government is requesting a complete data package that will enable any form of independent analysis including failure analysis of parts as well as long-term obsolescence management. The data listed will be used by the Gov evaluation team to assess the implemented quantitative assurance techniques, process flows developed and best practices implemented. The list should be further refined in the your Phase 1 SOW, metrics and/or deliverables.
    .

63. **Question**: Section 10.b.ii.5 (page 11, Mandatory Compliance with Restrictions: Can the Government please specify how these requirements apply? As indicated previously, these requirements are dictated in a vacuum without regards to project performance or any reference to data controls or categories.

    Response: The respondents should read DoDI 8582.01 and DoDM 5200.01 Volume 4 for compliance.

64. **Question**: Section 10.b.ii.8 (page 12): Please clarify what deliverables the Government will be using to base assertions. Also, no long-term sustainability objectives are provided so that offerors can meaningfully address them in their bids.

Response:

a. Data rights should be part of the technical response per section 10.b.ii
b. The desire at FOC is that this investment will enable a self-sustainable commercially owned and operated capability.

65. Question: Section 10.b.ii.8.b (page 12): Can the Government provide, as a representative example, what form and content is necessary to provide an adequate rationale?

Response: There is no specific form or content required to provide rationale. Proposal assertions that merely state lesser rights without explanation will not be evaluated as meeting the requirement. 48 CFR § 252.227-7017 could be used as a guideline.

66. Question: Section 10.b.ii.8.d (page 12): In stating all applicable software licenses must be identified and included with the response do you mean the full text of the software license agreements are to be included, and counted against the page count? May offerors provide links to widely available terms? For example, open source software terms are generally available, as are many commercial licenses. To accelerate proposal preparation, please consider alternatives to providing physical copies of the license with the response.

Response:

a. The respondents are permitted to provide detailed software licenses as attachments that do not count against the page count.
b. Linking to a widely use/publicly available license is acceptable as the commercial links only contain the license information and are not used as extensions of their technical proposal.

67. Question: Section 10.b.iii.6 (page 13): Please specify the Government's core technical objectives. There are no core or desired, objective or threshold, objectives listed in the RFS. Offerors do not have a meaningful basis on which to propose without better definition of those aims.

Response: Phase I and Phase 2 objectives are specified in RFS. The desire at FOC is that this investment will enable a self-sustainable commercially owned and operated capability.

68. Question: (Multiple) Can the Government please specify ratings criteria for each technical factor? Section 10.c, page 13 Can the Government specify what it means to be most advantageous in relation to technical and cost factors? Section 10.d, page 13

Response:

a. The Government will not be providing ratings criteria
b. The Government will evaluate each proposal to select best interest of the Government

69. Question: Section 15.f, page 15 Submissions to the RFS should be protected consistent with the Procurement Integrity Act per 10 USC 2371b(h). It is improper for the agency to apply only a 5-year protection period to submissions (this is not a CRADA under 15 USC 3710a). Please clarify that

proposal information will be returned or destroyed, handled consistently with the Procurement Integrity Act, and not subject to FOIA? Please also specify how proposals are to be marked to ensure such handling?

Response: Markings are the responsibility of the company submitting the information. Data will be protected in accordance with the marking of the materials. If information is identified as proprietary/confidential, the information is exempt FOIA.

70. Question: (Multiple) Need clarification of the following statement: All prospective respondents must be members of the NSTXL consortium. Does this mean the prime or lead respondent or does this include all team members included in a specific response?

Response: If there is teaming on the solution, only the Prime/Lead Respondent needs to be a member of the consortium.

71. Question: Are providers of software solutions (EDA, Yield Analysis, Design/IP management or otherwise) required to be U.S. based firms?

Response: No, while preferred and desired, it's impractical to enforce. Even those that are US based depend on international software development teams. Some Application Engineering support may be limited to US citizens.

72. Question: (Multiple) Section 9 states that at a minimum the Government is requesting the delivery of all intellectual properties (IPs) developed during and used for the project. Will the DoD be willing to work with commercial non-traditional government contractors who would seek to leverage and adapt their commercial technology which incorporates intellectual property that was developed at private expense, that would need to be retained by those non-traditional commercial companies? As currently presented, the IP requirements specified herein will sacrifice many of the technical objectives for this project. If the Government desires the best commercial technologies, the Government should not include IP as an evaluation factor while also indicating its only desire is government purpose rights.

Response: We are only asking for rights to data first created under the project, so pre-existing rights would be negotiated. The government is requesting a complete data package that will enable any form of independent analysis including failure analysis of parts as well as long-term obsolescence management. Generally speaking, our requested data rights are flexible, and any offeror can suggest rights that they think are appropriate. While a minimum set of IP rights to info that we feel is critical, we will leave open the possibility of negotiating changes before phase 2. IP will remain an evaluation factor based on value. Better data rights would not automatically result in a winning proposal. (But all else equal, a proposal with better rights should win.)

73. Question: Section 10 b. iii. states that the Price Response has a max page limit of 5 pages. The RFS also recommends supporting BOE pricing information and states that the respondent shall delineate key pricing components & show clear traceability back to the phases and/or milestones of the Technical Response. Can this page limit be exceeded without being rejected and deemed ineligible for consideration of an award?

Response: "No, page limit should not be exceeded"

74. **Question**: (Multiple) Section 11 a. lists three Evaluation considerations. Are these three evaluation considerations weighted or are they equal? Can the Government provide, as a representative example, what form and content is necessary to provide an adequate rationale?

Response: The Government evaluation team will evaluate proposed solutions. The guidance in Section 11 is all that will be provided.

75. **Question**: In Table 2 of the RFS (pg.5), how is the quantity of total designs per year (for both IOC and FOC) split across the digital and mixed signal design categories?

Response: This will be driven by DoD program requirements and DIB system development needs. The intent of RAMP is to establish a process flow for both of these areas. Quantities or mix cannot be predicted.

76. **Question**: Would creation of a university-affiliated research and development entity (similar to USC ISI or CMU SEI) focused on advanced assured microelectronics that provided design services to DIB companies and DoD be inside the scope of the program?

Response: All proposal will have to meet the requirements in the RFS, including a sustainable business model as a service provider. All proposals will be considered fairly.

77. **Question**: (Multiple) What is the anticipated award date?

Response: Sometime in July.