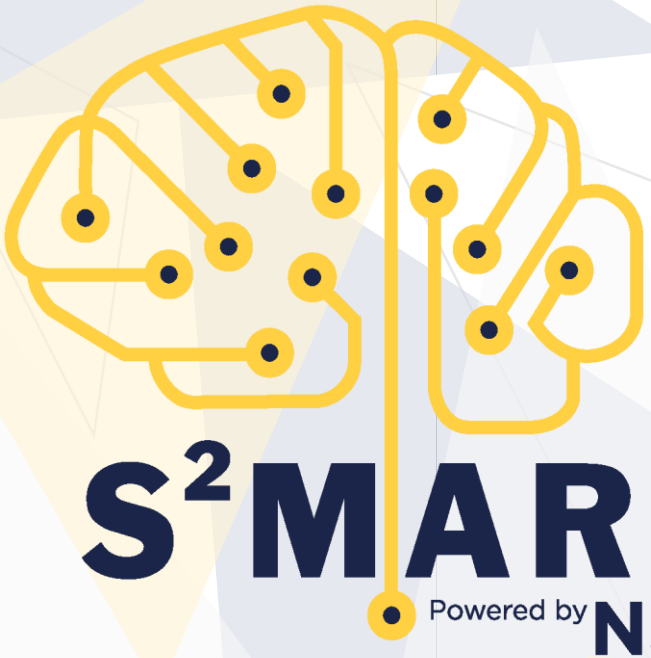


S²MARTS

Powered by NSTXL

WELCOME to PROJECT TALX

Transparent Accessibility • Live Exchange

April 30, 2020
3:00PM (EDT)

Slido Event Code (for Q&A): E046

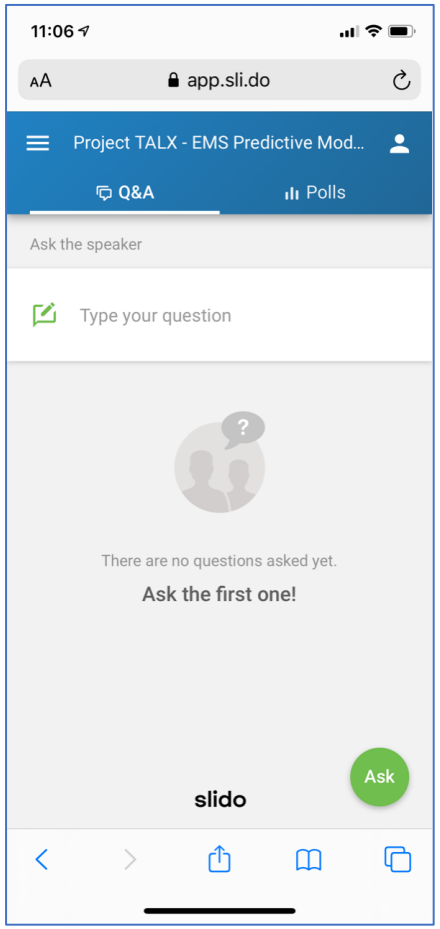
About the Q&A

Q&A Review Process

1. Questions will be submitted via Slido.com
2. Join Slido by going to Slido.com on your phone or laptop and entering this event #: **E046**
3. Questions will be captured and shared with the audience

Welcome Page

Phone App



Interested in submitting a question?
Go to **www.slido.com** and enter the following event code: E046

S²MARTS

Speaking Today

- **Ms. Brooke Pyne** | Director, S²MARTS
- **Mr. Iain Skeete** | Acquisition Principal, NSTXL
- **Ms. Nicole Petta** | Assistant Director for Microelectronics, DoD, OUSD for R&E
- **Mr. Brett Hamilton** | Distinguished Scientist for Trusted Microelectronics, NSWC Crane
- **Mr. Karl Franklin**| Technical Lead, NSWC Crane
- **Mr. Matt Sale**| Technical Lead, NSWC Crane

Interested in submitting a question?
Go to **www.slido.com** and enter the following event code: E046

S²MARTS

Webinar Agenda

Project: 20-06 - Rapid Assured Microelectronics Prototypes (RAMP) using Advanced Commercial Capabilities

- Rules of Engagement
- Project Discussion
- Q&A Open Exchange via Slido.com

Interested in submitting a question?
Go to **www.slido.com** and enter the following event code: E046

S²MARTS

Rules of Engagement

- Remember the intent
- Not intended to vet your specific solution
- Primarily a programmatic/technical conversation
- Any discrepancies? Documentation takes precedence
- Time permitting, all questions will be answered

Interested in submitting a question?
Go to **www.slido.com** and enter the following event code: E046

S²MARTS

Government Project Leads

Project: 20-06 - Rapid Assured Microelectronics Prototypes (RAMP) using Advanced Commercial Capabilities

- **Ms. Nicole Petta |** Assistant Director for Microelectronics, DoD, OUSD for R&E
- **Mr. Brett Hamilton |** Distinguished Scientist for Trusted Microelectronics, NSWC Crane
- **Mr. Karl Franklin |** Technical Lead, NSWC Crane
- **Mr. Matt Sale |** Technical Lead, NSWC Crane
- **Mr. Shaun Davis |** S^2MARTS PM Team, NSWC Crane
- **Mr. Bryan Smith |** S^2MARTS PM Team, NSWC Crane
- **Mr. Dallas Parsley |** Agreements Officer, NSWC Crane
- **Ms. Mary Beth McFann |** Agreements Specialist, NSWC Crane
- **Mr. Eric Vanwiltenburg |** Legal Counsel, NSWC Crane

Microelectronics

Nicole Petta
Assistant Director (AD) for Microelectronics

Microelectronics overview

Purpose

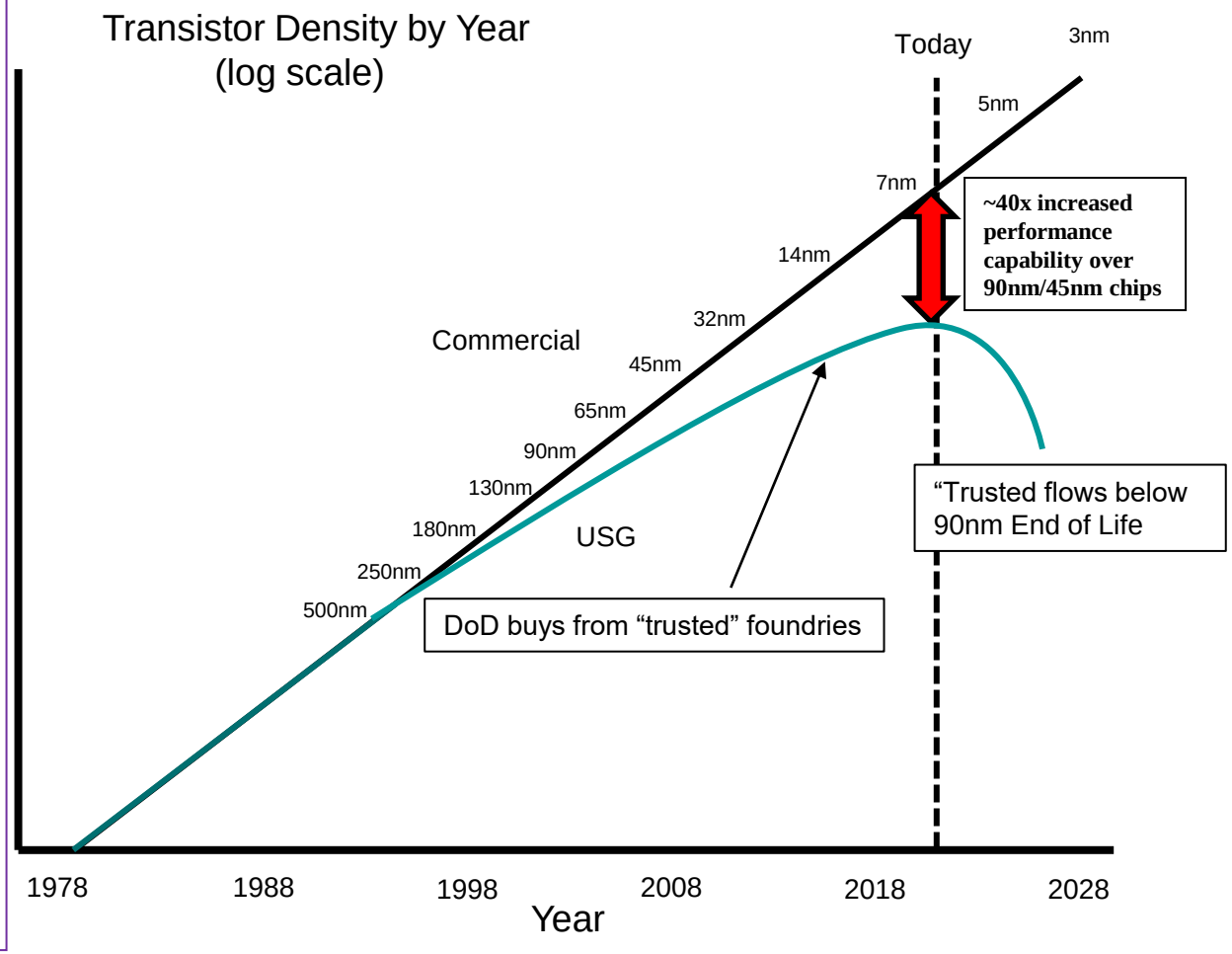
- DoD must rapidly pursue an alternative microelectronics security framework that emphasizes flexible access to the commercial sector with high levels of security.
  - Multiple commercial partners for securing custom microelectronics
  - Focused on leading-edge commercial capabilities
  - Flexible, adaptive and responsive to new threats
  - Deliver capabilities and protections and apply selectively based on program requirements

OSD Microelectronics Roadmap Categories

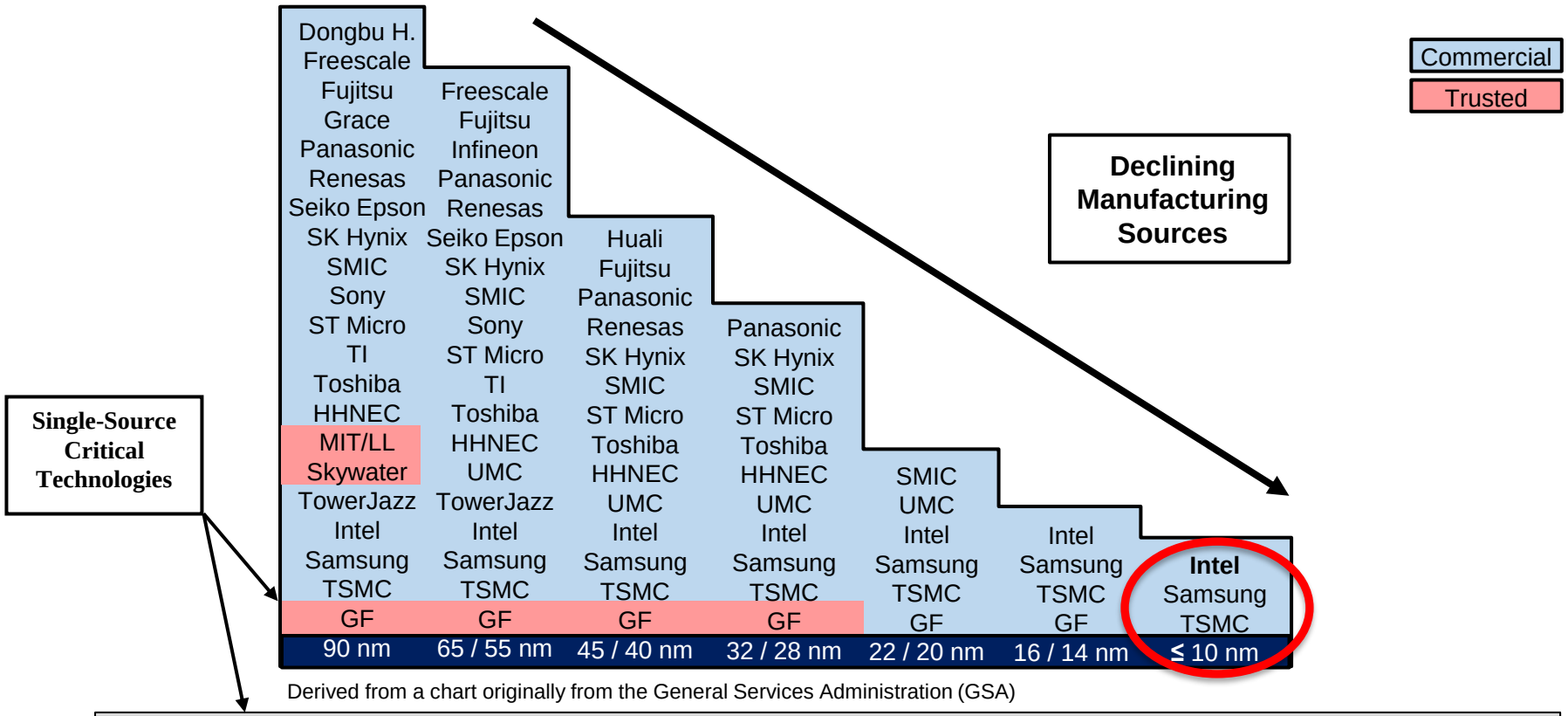
- **Access to State-of-the-Art (SOTA) Microelectronic Integrated Circuits (SoCs)**
- **Access to SOTA Microelectronic Packaging and Test**
- **Access to Advanced DoD Unique Microelectronics Technology**
  - **Radiation-Hard Microelectronics**
  - **Non-CMOS Microelectronics**
- **Supply Chain Awareness and Security**
- Education & Workforce Development
- Trusted Foundry and Obsolescence
- Disruptive Research and Development

Current regulations intended to prevent the proliferation of defense-related technologies have prevented DoD from fully leveraging on-shore SOTA manufacturing capabilities.

- **Currently DoD uses a "perimeter" approach to security.**
  - Perimeter approach is incompatible with commercial practices.
  - The result is that SOTA fabrication facilities will not become "trusted".
- **The result is that DoD does not have access to the best technology.**
  - ~ 40X less performance and 30X lower density of transistors.
  - DoD system capabilities are severely limited by the lack of CSWaP.



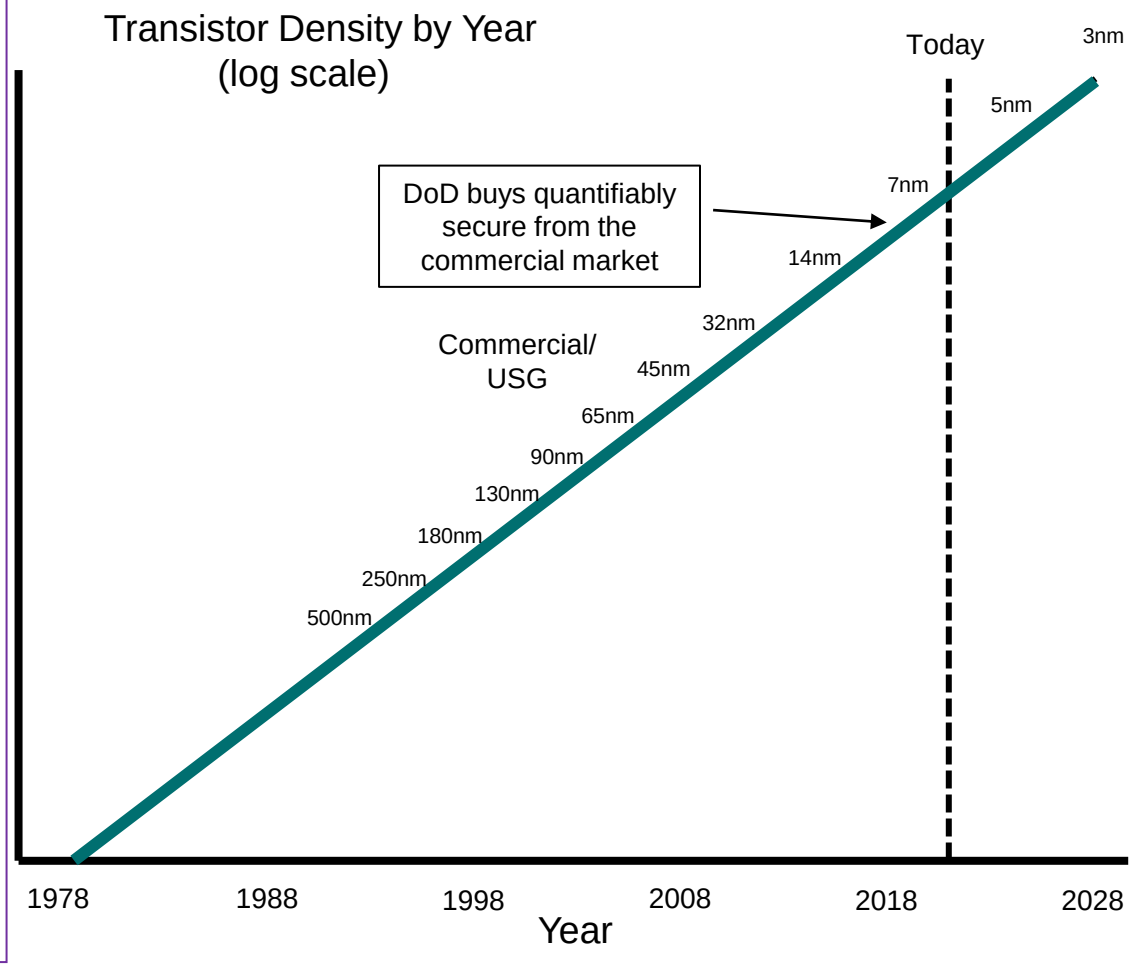
DoD requires a multi-vendor, assured, pipeline for critical microelectronics in a diminishing global supply chain



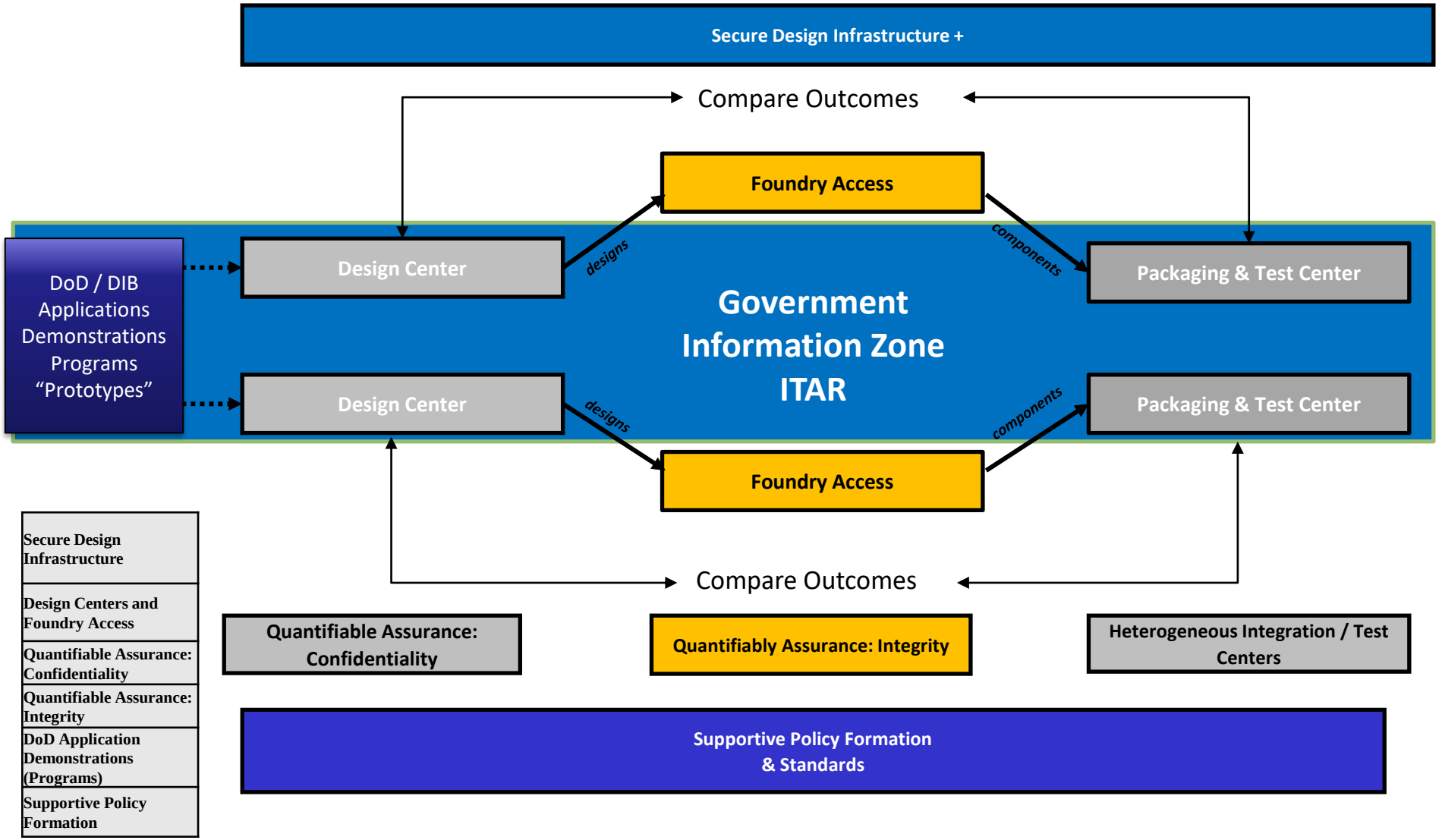
Derived from a chart originally from the General Services Administration (GSA)

The goal is for DoD to have measurably secure access to multiple SOTA fabrication capabilities that scale with commercial

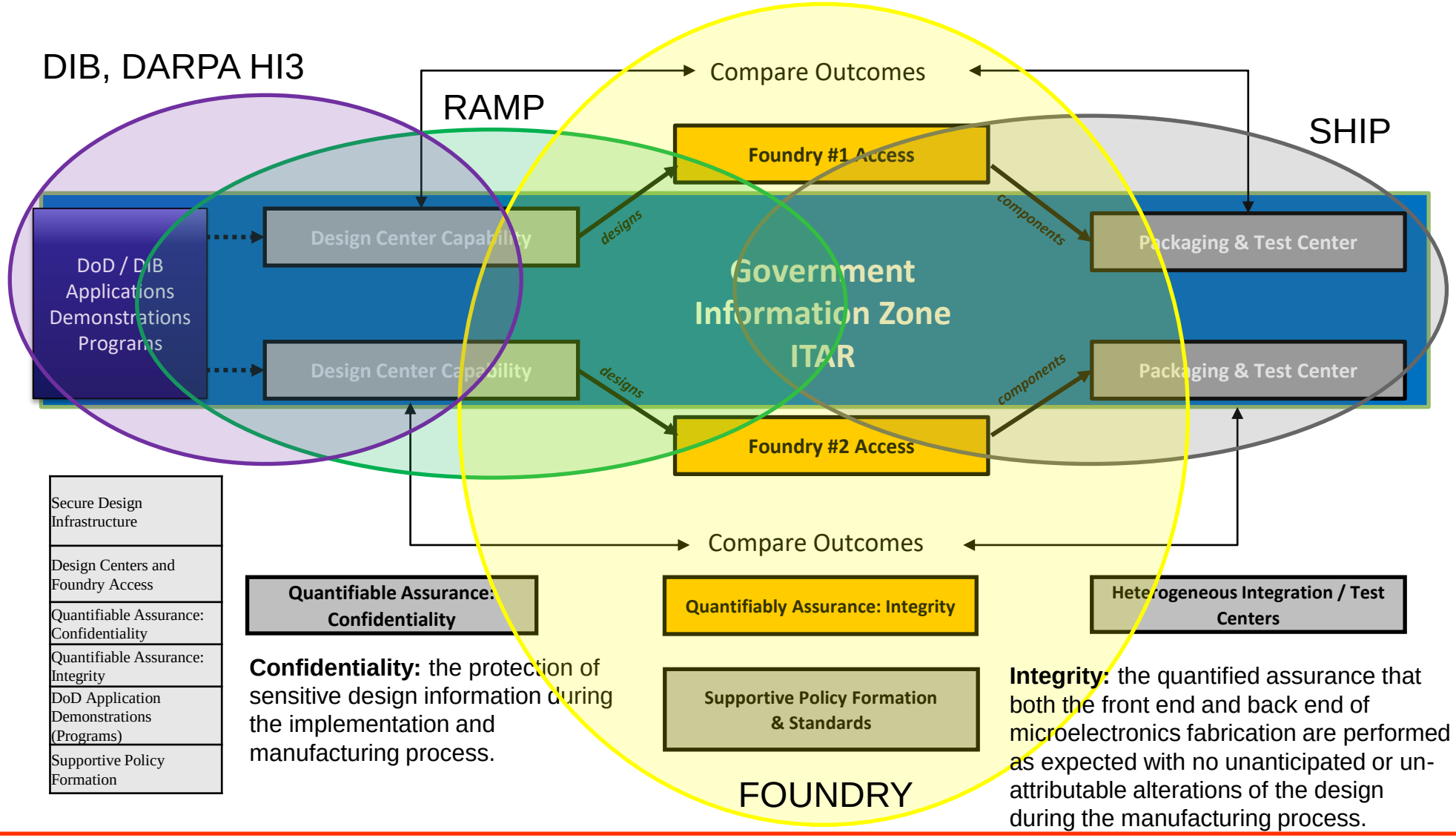
- **DoD will discard the "perimeter" approach to security and adopt a "zero-trust" methodology instead.**
  - Risk-management-based approach to security along the entire life-cycle, informed by data, not perimeters.
- **DoD will get back on the commercial curve.**
  - DoD cannot afford to be excluded from SOTA capability.
  - Relying on old technology does not make us secure.



Lifecycle Quantifiable Assurance:
Quantifiably "Secure" design data + Manufacturing process data + Test data = Risk



Rapid Assured Microelectronics Prototypes using Advanced Commercial Capabilities (RAMP) and State-of-the-art (SOTA) Heterogeneous Integrated Packaging (SHIP) Process Flow

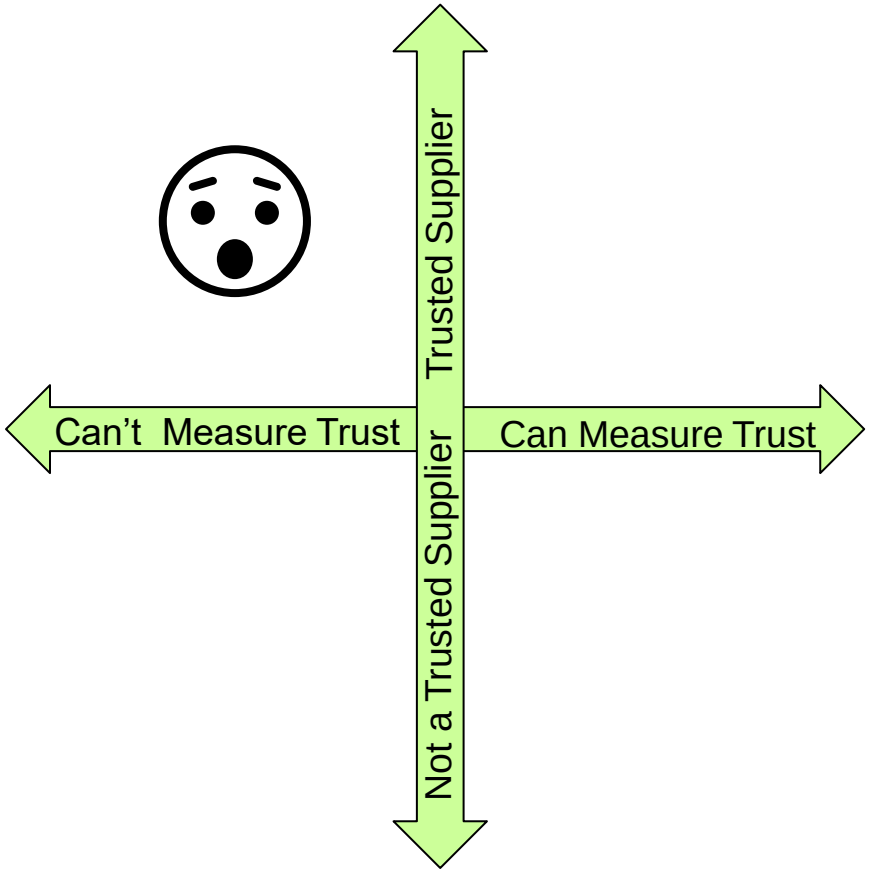


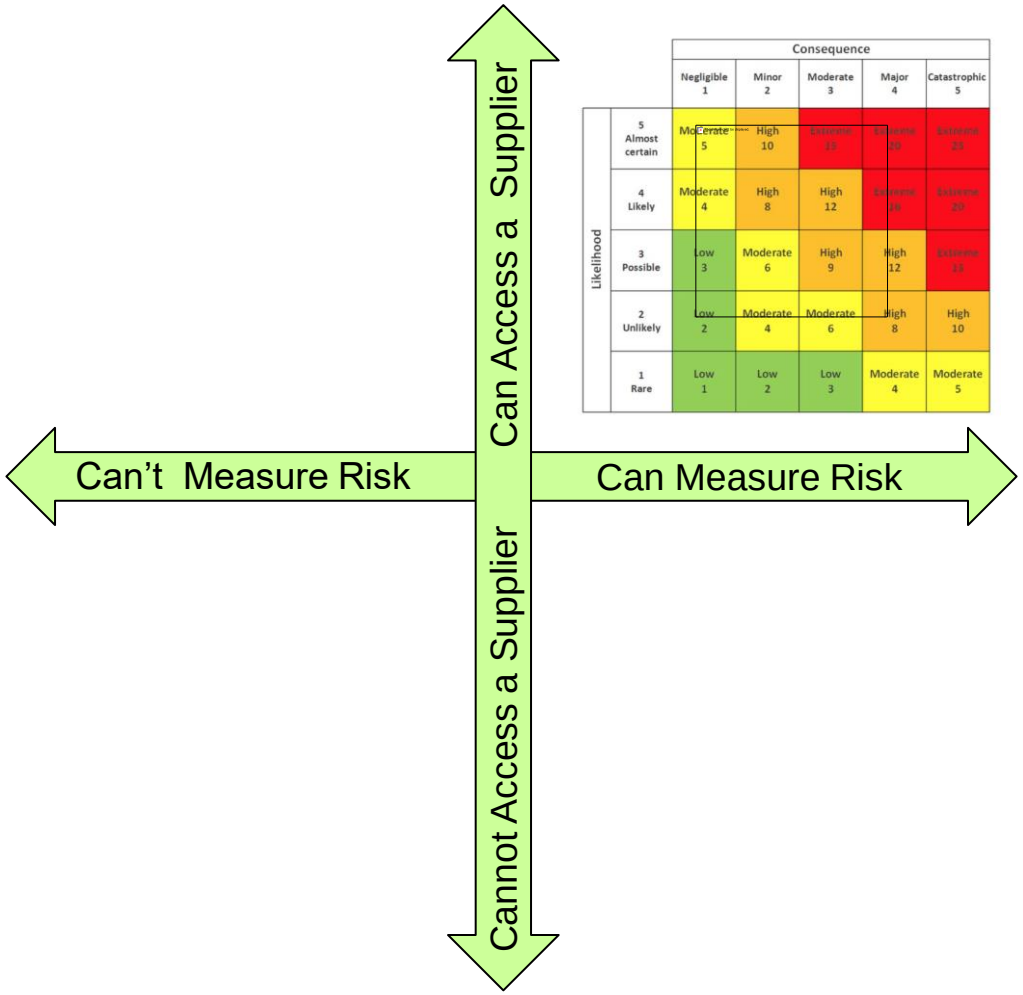
Secure Design Infrastructure
Design Centers and Foundry Access
Quantifiable Assurance: Confidentiality
Quantifiable Assurance: Integrity
DoD Application Demonstrations (Programs)
Supportive Policy Formation

Confidentiality: the protection of sensitive design information during the implementation and manufacturing process.

Integrity: 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.

Trust vs. Zero-Trust





NDAA Language: Requires Defense Microelectronics Products and Services Meet Trusted Standards (Sec. 224):

- The NDAA instructs DOD to ensure, by January 1, 2023: Microelectronics purchased by DOD meet certain supply chain and operation security standards.

- The standards, which must be developed by January 1, 2021, will systematize best practices relevant to (1) manufacturing location, (2) company ownership, (3) workforce composition, (4) access during manufacturing, suppliers' design, sourcing, packaging, and distribution processes, (5) reliability of the supply chain, and (6) other matters germane to supply chain and operational security.

- Additionally, the NDAA directs DOD to consult with microelectronics suppliers and representatives of the defense industrial base in developing these standards and to ensure to the greatest extent practicable that microelectronics suppliers can sell these same products commercially.

What We Are Seeking

- The RAMP prototype will 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 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 ≤ 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

Phased Approach

- **Phase I (6 months)**
  - **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.**
  - **Application of methods to ensure both the confidentiality and integrity of circuits during the manufacturing flow.**
  - **Definition of a DoD supply chain standard that leverages commercial microelectronics supply chain security methods to meet DoD needs.**

- **Phase II (18 months)**
  - **Demonstrate the implementation of the capabilities developed in the Secure Design Capability and confidentiality and integrity developed in Phase I.**
  - **Demonstration of the secure design capability and implementation of quantifiable assurance technology**

Questions & Answers

- Today's topics will be captured in Q&A posting on S2MARTS.org
- Reminder: Any changes will be publicized via RFS modification
- Slido Event Code: **E046**

Interested in submitting a question?
Go to **www.slido.com** and enter the following event code: E046

S²MARTS

Question 1

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

Answer: 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 off-shore foundries are not a focus of this at present, they should not be excluded from consideration. Demonstration of quantifiable assurance capabilities that could enable the use of offshore foundries would be advantageous.

Interested in submitting a question?
Go to **www.slido.com** and enter the following event code: E046

S²MARTS

Question 2

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?

Answer: The DoD is looking toward utilizing assurance technologies with the greatest flexibility for access to State-of-the-Art (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).

Interested in submitting a question?
Go to **www.slido.com** and enter the following event code: E046

S²MARTS

Question 3

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?

Answer: 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). Additional reference Instructions and Documents will be provided in writing.

Interested in submitting a question?
Go to **www.slido.com** and enter the following event code: E046

S²MARTS

Question 4

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

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

Interested in submitting a question?
Go to **www.slido.com** and enter the following event code: E046

S²MARTS

Question 5

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?

Answer: 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.

Interested in submitting a question?
Go to **www.slido.com** and enter the following event code: E046

S²MARTS

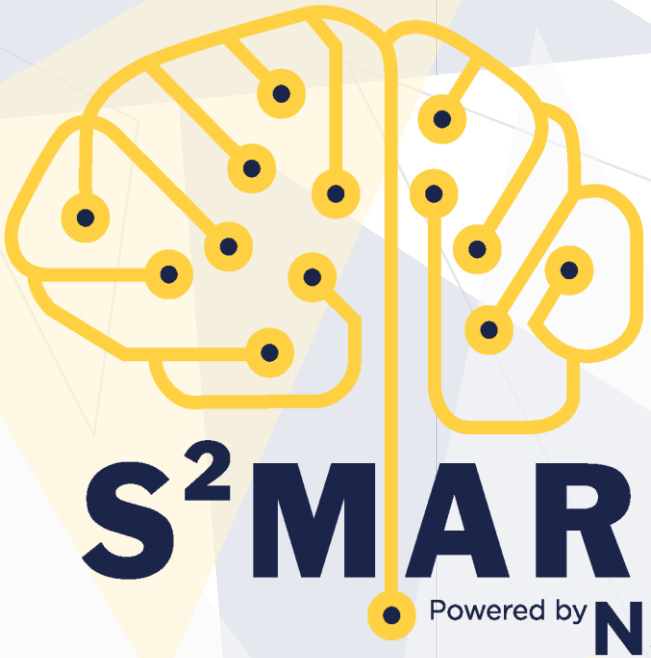
Question 6

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

Answer: 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."

Interested in submitting a question?
Go to **www.slido.com** and enter the following event code: E046

S²MARTS



Open Exchange

Slido Event Code: E046

Closing Reminders

- All Q&A's are publicly available – visit S2MARTS.org
- Proposals are due on **May 29th, 2020 NLT 12 PM EDT.**
- Follow the instructions within the Request for Solutions
- Ensure your membership is active
- Engage with other potential partners using NSTXL Community

S²MARTS Team

Director
brooke@nstxl.org

Specialist
janay@nstxl.org

Membership
membership@nstxl.org

S²MARTS

Thank you for joining Project TALX!