# Trusted Microelectronics Workshop:

# "Trusted Microelectronics: The Industry's Perspective"

**February 3, 2016**

**Hosted by the National Defense Industry Association (NDIA) Event 6290**

# Acknowledgments

This workshop came together with the help of a number of important people. Ms. Britt Sullivan and Ms. Rebecca Danahy of the NDIA did a great job organizing and hosting the event. Mr. Joseph Spruill and the Lockheed Martin Corporation Global Vision Center staff are thanked for providing a wonderful site to hold the workshop. Thanks to the keynote speaker Mr. David Sobczak, Director, Program Management, GLOBALFOUNDRIES Aerospace & Defense Business Unit and GLOBALFOUNDRIES United States 2 (GFUS2) Trusted Production Officer for introducing the GFUS2 Trusted Foundries to the meeting participants and providing insight to the GLOBALFOUNDRIES business model. Many thanks for the valuable perspective offered by the systems integrators' panel members that included Charley Adams, Northrop Grumman; Pat Hays, Boeing; Mitch Meinhold, Lockheed Martin; Mark Porter, General Dynamics; and Jessica Denham, Raytheon. The DMEA Trusted Accredited Suppliers panel provided beneficial insight to the challenges faced by the supplier community; representatives included Wayne DeCarlo, Photronics; Scott Jordan, Jazz Semi Trusted Foundry; Stewart Ocheltree, BAE Systems; and Kirk Peterson, ON Semiconductor

Once again, attendee participation was key to the workshop's success, so thanks to the many participants who were very active in the event discussions. Finally, the efforts of Dr. Brian Cohen (IDA), Mr. Sydney Pope, Decisive Analytics Corporation (DAC), and Ms. Catherine Ortiz, Defined Business Solutions, are appreciated for organizing the event and ensuring that the workshop ran smoothly.

# Contents

# 1. Introduction

The NDIA Trusted Microelectronics Workshop series was launched in 2013 to provide an open forum for government and industry to discuss microelectronics supply and security issues related to defense and national security systems. The initial workshop held in June 2013 explored how to make the Department of Defense (DoD) Instruction 5200.44 a success.[1] The report from that meeting recorded a strong desire by the participants to follow up that first workshop with similar events.[2]

A subsequent meeting was held in January 2014 with the theme of "Trusted Microelectronics for Systems Security."[3] The report from that meeting discussed a number of areas identified for further discussion including opportunities for managing supply chain risk beyond Application Specific Integrated Circuits (ASICs) and opportunities for cost-effectively leveraging industrial capabilities.[4]

In August 2014, the third Trusted Microelectronics Workshop explored the overlap between the requirements of safety, quality, and security in aerospace and defense systems.[5] The report from that meeting included good approaches discussed by the audience on how to leverage existing quality and safety disciplines to address supply chain security risks.[6]

The fourth Trusted Microelectronics Workshop,[7] held in February 2015, was designed to consider hardware assurance challenges in a system's sustainment phase, as components are more difficult to get from the original suppliers. The report from that workshop included discussion on how sustainment managers and representatives from the Diminishing Manufacturing Sources and Material Suppliers (DMSMS) community are using trusted and trustworthy suppliers to mitigate electronic component risks later in the

---

[1] NDIA Event 3180 - Trusted Microelectronics Workshop

[2] Trusted Microelectronics Workshop: "Making 5200.44 a Success," Report on the NDIA Workshop 3180, June 28, 2013

[3] NDIA Event 4290 - Trusted Microelectronics Meeting

[4] Trusted Microelectronics Workshop: Trusted Microelectronics for Systems Security, Report on the NDIA Workshop 4290, January 15, 2014

[5] NDIA Event 487E - Trusted Microelectronics Meeting

[6] Trusted Microelectronics Workshop: "Connecting Safety, Quality and Security: The Benefits of Trusted Microelectronics," NDIA, August 21, 2014.

[7] NDIA Event 587D - Trusted Microelectronics Workshop

lifecycle.[8] The audience asked for better definition of the DMSMS problem, identification of stakeholders, and development of the process to get systems engineers and supply chain managers to address security risks early in the component selection process.

The fifth Trusted Microelectronics Workshop[9], held on August 25, 2015, looked to the future.[10] Specifically, how the DoD could satisfy the need for trusted microelectronics in an increasingly globalized integrated circuit industrial base. With a theme of Trusted Microelectronics: The Future Landscape, the workshop was advertised publicly on the NDIA website and featured Government to discuss the work being done to ensure Government programs have choices for leading edge microelectronics technologies that are trustable. Mr. Robert Gold, Director, Engineering Enterprise ODASD(SE) provided the keynote address. The audience asked for the next workshop to offer Industry an opportunity to respond to the Government plans discussed in the August workshop.

The most recent Trusted Microelectronics Workshop[11], held on February 3, 2016, was organized to give Industry an opportunity to respond to the Government plans for assuring access to Trusted Microelectronics and to raise issues that they face as they build defense systems. The event was advertised publicly on the NDIA website with the following description:

*NDIA is pleased to offer our sixth workshop designed to identify ways in which Trusted Microelectronics can contribute to greater systems security and information assurance. With participation from both Government and Industry, our workshops have provided an effective forum for direct discussions of the challenges faced by policy makers, program managers, systems developers, and supply chain managers.*

*In our last workshop, we heard from Government experts on their activities to ensure defense and national security systems have the protection of Trusted Microelectronics. Now its Industry's turn to talk about their Trusted offerings and what can be done to increase the use of Trusted Microelectronics.*

*At this workshop Industry experts will discuss the work being done to ensure:*

- *Government programs have choices for leading edge microelectronics technologies that are trustable*

---

[8] http://www.ndia.org/Divisions/Divisions/SystemsEngineering/Documents/NDIA Trusted MicroE Workshop Proceedings Feb 2015.pdf," NDIA, February 26, 2015.

[9] NDIA Event 5290, Trusted Microelectronics: The Future Landscape

[10] http://www.ndia.org/Divisions/Divisions/SystemsEngineering/Documents/NDIA Trusted MicroE Workshop Proceedings Aug 2015.pdf," NDIA, August 25, 2016.

[11] NDIA Event 6290, Trusted Microelectronics: Industry's Perspective

- *State-of-the-art technologies critical to national defense programs are available from domestic sources*
- *R&D in technologies that ensure Trust are part of microelectronics suppliers' development roadmaps*

*David M. Sobczak, Director of Program Management within the Aerospace and Defense business unit of GLOBALFOUNDRIES, will provide the keynote address.*

*Program representatives from General Dynamics, Raytheon, Boeing, Northrop Grumman and Lockheed Martin will describe the factors that influence their decisions to either use a Trusted Accredited Supplier for microelectronics, to purchase components from other sources or to use COTS components.*

*The DMEA Trusted Accredited Suppliers will provide information on their Trusted offerings and future development plans.*

*Our workshops are designed to be truly interactive with full participant engagement. Plenty of open discussion time is scheduled throughout the day. Please join us to learn about Industry's perspective on Trusted Microelectronics and to add your voice to the conversation.*

*Who should attend: Government and Industry program managers, systems engineers and developers, systems security engineers, microelectronics policy makers, supply chain and sustainment officials, information security managers, and purchasing and procurement professionals.*

Dr. Brian Cohen, an IDA Research Staff Member, opened the workshop with an introduction to the day's theme of exploring issues revolving around the future for trusted microelectronics. He thanked Lockheed Martin for the use of the facility and to NDIA for hosting. Dr. Cohen notes that this is the sixth Trusted Microelectronics Workshop and is especially pleased that this event will include views from people who buy microelectronics for government systems. He stated that the landscape for microelectronics continues to migrate away from U.S. soil. Because of this shift, defense contractors are faced with an increasing challenge to ensure their systems will perform as required when required. Dr. Cohen concluded his opening remarks by encouraging contributions from all and a reminder that comments are for non-attribution.

Mr. David Sobczak, Director, Program Management, GLOBALFOUNDRIES Aerospace & Defense Business Unit and GLOBALFOUNDRIES United States 2 (GFUS2) Trusted Production Officer provided the keynote address and expressed his appreciation for the opportunity to introduce GFUS2.

Following Mr. Sobczak's presentation, Mr. Sydney Pope, a DAC Systems Security Specialist, moderated a discussion on the leverage points that Mr. Sobczak introduced in his keynote.

After a break, we heard from a panel of representatives from DMEA Trusted Accredited Suppliers that consisted of Wayne DeCarlo, Photronics; Scott Jordan, Jazz Semiconductor Trusted Foundry; Stewart Ocheltree, BAE Systems; and, Kirk Peterson, ON Semiconductor

Following the Trusted Accredited Suppliers panel, Dr. Brian Cohen, moderated a discussion that expanded on the issues raised by the panel.

After a lunch break, participants heard from a panel of defense systems manufacturers; those people who work with the government program offices to determine if Trusted Accredited Suppliers are required for the program's mission assurance. The workshop participants heard valuable perspective from Charley Adams, Northrop Grumman; Pat Hays, Boeing; Mitch Meinhold, Lockheed Martin; Mark Porter, General Dynamics; and Jessica Denham, Raytheon.

Following the Defense Systems Manufacturers panel, Mr. Syd Pope, moderated a discussion that expanded on the issues raised by the panel.

Dr. Cohen moderated the final open discussion during which the participants asked for working groups to be formed to address issues raised during the day. The full agenda is shown in Appendix A. The keynote presentation from Mr. Sobczak is in Appendix B. The registration roster is provided in 3.Appendix C.

# 2. Minutes of the Workshop

On Tuesday, February 3, 2016, the NDIA sponsored a Trusted Microelectronics Workshop, with technical co-sponsorship by the Trusted Accredited Suppliers Steering Group, at the Lockheed Martin Global Vision Center, Arlington, Virginia. Ninety-six individuals from government and industry attended. A copy of the Agenda is in Appendix A. The Workshop began at 8:30 a.m. and adjourned at 3:30 p.m.

## Welcome

*Dr. Brian Cohen, IDA Research Staff Member*

Dr. Cohen kicked off the workshop by describing its goal and then introducing the keynote speaker, Mr. David Sobczak.

## A. Trusted Microelectronics: Introducing GFUS2

*Mr. David Sobczak, Director, Program Management, GLOBALFOUNDRIES Aerospace & Defense Business Unit and GFUS2 Trusted Production Officer*

Mr. Sobczak gave a candid and insightful view of GLOBALFOUNDRIES business, products and strategy. Throughout the presentation, Mr. Sobczak emphasized the company's commitment to growing their microelectronics business and to the Trusted Foundry Program.

**Company Overview and Industry Position**

- Noted in 2015, over $120B in acquisitions in the semiconductor industry; more than twice the amount of acquisitions combined in the last 5 years
- GF is largest privately held semiconductor company and the second largest pure play foundry company
- GFUS2 could be viewed as a 7-year start-up; 2010 Charter acquisition gave GF traditional foundry capabilities
  - 2012 Malta facility came online; Dresden shifted focus to IoT technologies
  - Locations: Burlington (Fab 9), East Fishkill (Fab 10), Malta (Fab 8), Singapore (Fabs 2-7) and Dresden (Fab 1)

- With the acquisition of IBM's semiconductor business, GFUS2 keeps the people, the parts and the customers
  - Added 5,000 employees to GF base
  - Dynamic has changed with increased capacity; GF is able to offer wide range of product offerings with two pure play foundries and full spectrum of technologies
  - IBM was focused on financial performance; GF is focused on growth
  - Diversification is important, as is reaching across markets with range of technologies

**Market and Business Unit Structure**

- Factors considered for growth:
  - Consumer wireless, mobile computing, phones
  - Internet-of-Things expected to be the next big thing
  - Routers, TVs, base stations
  - High Performance computing
  - Aerospace & Defense (A&D) and Industrial are new markets for GF; looking for growth opportunities in these markets
- ASIC and RF business units are mostly from IBM
  - A&D BU is product agnostic; not too different from the IBM days, from the Trusted perspective and security operations.
  - There is a "double-dose" of Trust; the same business structure that created the Trust accreditation is in place for maintaining Trust

**Trusted Technology Offerings**

- Products organized by DMEA matrix; portfolio available through TAPO
- Packaging done at Bromont, CA; provides service as Trusted broker
- Offer end-to-end flow for commercial, ITAR and Trust
  - Commercial business has significant security controls because customers entrust the fab with their Crown Jewels; it is a misperception that the commercial business has loose security
  - ITAR is another step up from commercial and may be option for defense systems that are not required to have full Trust

**New Hybrid Trust Model for Advanced Nodes**

- Uses a Trusted flow until its time to use a fab, then enter a Trusted flow again after fabrication
  - Fabs these days are very automated and security has increased (even in commercial) and that commercial controls could be secure enough
- Could work in Malta but people will have to get comfortable with the concept

**Viability of "split fab" concept for Trust**

- IBM and GF successfully proved concept for IARPA
  - GF is interested to be able to pull Dresden and Singapore facilities into model
  - Technology exists but business case has not been established and may be harder to prove
    - What is the ROI?
    - What are requirements (EDA flows, design kits, etc.)?
    - What about warranties and other technology qualifications?
    - IP qualifications? (IP, compilers, etc.)
    - Will volume be sufficient for acceptable yields
  - Even if government provides all funding there is still opportunity cost
    - All IP would have to be requalified; who will own it?

**2.5D TSD Si Interposer**

- Conceptual chip architect using Trusted and non-Trusted parts
- Takes advantage of technology without exposing IP

**Summary**

- GLOBALFOUNDRIES is committed to the Trusted Foundry Program
- Driven to grow the business of Trust
- Looking to increase security scope at Malta plant but will not be fully Trusted
- May 3-4$^{th}$, Trusted Foundry Advanced Technology Training in Burlington; registration is open now

***Question:*** Will commercial fabs look into becoming Trusted? What about Trust for other industries like automotive?

- The concern is there, they are not likely to get all the way Trusted, but they are increasing security for sure
- Commercial products are tightly controlled because of company's IP and the associated risks

***Question:*** What is GFUS2 doing to allow long term access to Trusted products/partners?

- Answer: current contract setup is actually better than the agreement set up previously with IBM; if the business grows, the contracts will continue to be extended
- The current contract is unilaterally extended through summer of 2017, contract is being worked on for beyond at this time

***Question:*** What, in your opinion, is driving company consolidation and why so much of it?

- Answer: There is a lot of cash available in the leading companies, $700B in the technology sector alone
- The uncertainty of the "next big thing" and the slow down of the smart phone market, makes acquisitions more attractive
- With cash on hand, it makes more sense to buy advanced technology than develop it

## B. Open Discussion

*Moderated by: Mr. Sydney Pope, DAC, Systems Security Engineering Expert*

An open discussion was moderated by Mr. Sydney Pope, a ODASD(SE) support contractor.

***Question:*** What are our choices for leading edge Trusted products? Responses included:

- There are only four advanced fabs in the world and we only have access to one: GLOBALFOUNDARIES
- Need robust Multi-Project Wafer program that closes the loop through design, mask and fab
  - Access to to advanced ICs is paramount; more important than malicious insertion risk
  - Commercial entities have high security practices built in to protect themselves and their customers; today's process control ensures Trust
  - With split fab and qualification an offshore foundry as Trusted, China will have access to the IP within weeks
  - 2.5 D package idea is a good place to start
  -

***Question:*** Should we invest in a National Foundry? How do we pay for it? Responses included:

- Incentivize companies to make purchases from current US fabs, to increase demand and growth
  - US needs to be able to offer best solutions.
- Can USG address issue of economies of scale?
  - The cost of everything, (from designs to masks, etc.,) is increasing
- FPGAs cannot be the answer because of battery consumption but are they part of the solution?
  - Though FPGAs are fast and cheap, ASICs ability to meet specific mission critical criteria are the only safe and secure option
- Consider a change in Program Management teaching and understanding that it would be less expensive to start in the acquisition and procurement planning and

plan for a lifetime buy (store the excess until needed) rather than have to go back and recreate a new, low volume wafer run

  - Today's acquisition policies do not support this approach; do they need to be changed?

- IP protection is more important than malicious insertion and prevention
  - Trust is critical to protect the capabilities of the product, keeping the CPI and IP secure
- What about design tools, can we qualify Trust through EDA tools?
  - There are too many variables to solely rely on EDA tools
  - Problems should be detected through distributed use – the greater number of people using the EDA tools, the more likely that problems will be discovered
  - The viability of design verification programs should be explored

## C. Panel Discussion: DMEA Trusted Accredited Suppliers

Mr. Sydney Pope moderated a panel of representatives from the DMEA Trusted Accredited Supplier companies and asked them to introduce themselves and provide a brief statement on their observations on the Trusted Supplier industry.

- Wayne DeCarlo, Photronics Inc
  - Photronics sees a very broad range of customer requirements particularly with protecting IP
  - Seeing now speed of execution time to market and monetization concerns
  - Doing a lot of mix and match between mature and high end within company
  - Highly motivated to stay Trusted
- Scott Jordan, Jazz Semiconductor Trusted Foundry
  - JSTF has access to all of Jazz's processes, they are both Category 1A/1B Trusted, SiGe SOI business is taking off
  - Customers want to use what is in place to control expenses with the exception of DARPA's unique requirements
  - Customers are asking for variations -- hybrid protection of certain components and capabilities
  - Doing a lot more Trusted work

- Stewart Ocheltree, BAE Systems
  - Rad hard IP products through TAPO, use GFUS2 to create products, supports continued access to advanced technology
  - Customers don't always know what to ask for; some customers want to be able to say they use a Trusted supplier but don't need the Trusted flow
  - Need to better communicate what Trusted means; more clarification and consistent understanding for the requirements of Trust.
  - People don't want to pay the cost for Trust unless it is required; if everyone wanted Trust it would be more cost efficient
  - Pretty comfortable with foreign made IP; always portions that are controlled at a very high level.
- Kirk Peterson, ON Semiconductor
  - #4 company in ASIC production
  - Efforts in the TASSG and the TFP has started to show as increase business and interest in Trust has grown
  - A minority of customers require full Trusted design

***Moderator Question:*** How has your product line evolved after becoming accredited? What are your customers asking for? Panelists responded:

- "ITAR plus" is what we are seeing from those that do not know about Trust, as our business models change, we are adopting to 'active design' so long as ROI is reasonable
- Customers are interested in using what is already in place and those are evolving as new processes are developed (through DARPA for example) pleased to see growth in Trust/trustworthy interest
- Customers are very conscious of costs and availability, but show more willingness to consider paying for Trust and security through ASICs

- We are surprised more customers don't know more about Trust, don't know to ask for it or what is involved.
  - Must request Trusted flow specifically, would love to see customers have a better understanding

***Moderator Question:*** How do you see your product offerings evolving? What does your roadmap look like from here? Panelists responded:

- Roadmap depends on customer demand, how far do they want Trust to run and working with them on what Trusted-flow is.
- Confusion between Trust and classified
  - Product offerings depend on classified versus unclassified Trusted flow; requests vary across the board, but many are embracing Trusted options
- Hybrid approach makes sense
  - Structured array approach may work for split fab without some of the obstacles; Triad does it today
  - Requiring clearances is problematic for lower level operators who don't want to go through the invasive security process -- Can we reduce the number of people who need to be cleared?
- Adding anti-tamper capabilities to the roadmap, achieving accreditation in test from DMEA, sees merit in split-fab approach
- At 28nm and below, NRE design costs are a consideration, though it will be difficult to find a Trusted fab at lower nodes

***Audience Question:*** What is a middle ground that the TASSG can develop, can this group create a buyer's guide with suggested language? Panelists responded:

- Agree that is something we have in line as a natural next step for us
- Included with the buyers guide we need to consider best practices, what the current threats are, and understand where the risks are
- The TASSG is great for the community, even though your company may be a competitor across the table, we all have common needs and this group is great to help find common ground – no company is only looking out for their own interests, the TASSG is really a successful collaboration

***Audience Question:*** Can you, as a group, recommend contract language to consider? This may provide greater clarity in requirements. Panelists responded:

- We have submitted suggested contract language to the DFARs that can be used to your needs; will share with the proceedings
- Audience member: The NRO just last month issued instruction to implement Trust and it is flowing down
- Ray Shanahan: The JFAC is interested in the language from the TASSG

## D. Open Discussion

Dr. Brian Cohen moderated an open discussion of the topics presented earlier:

***Moderator Question:*** ASICs account for 5-10% of DoD parts, what about the risks of the other 90%? How can we use Trusted for those risks? These risks may be more important for the catalog items than the traditional Trusted risks. What are the risks in the broader market and how can the Trusted accredited be used for that risk. Responses from participants included:

- We would need to find out what is the level of the risk? How does that part impact the entire system? How much cost is involved?
- There really is no silver bullet, nor is there one solution that we can use across the board
- Even if there are backdoors, unintentional threats, counterfeit and anti-tamper mitigations, the highest risk is in design stages and Trust is critical at that point
- Use an anchor component – a tamper resistant golden image
- Signal hardware root of Trust.
- Trusted design is important but will be accidental open doors.
- Can AT be deployed in the design? Tools are available.
- Counterfeiting is another major issue, overruns, reuse of used parts, etc. all need better regulations; government should stop using used parts

***Moderator Question:*** Should Trusted suppliers offer longer life options to prevent obsolescence? Should long-term availability be required? Responses from participants included:

- We need to consider the issue that we can be confident that there will be a supply available. (Michael Wynne (AT&L) letter)
- Need to be careful not to expand the Trust umbrella too wide
- It is cheaper to buy excess in the beginning than to go back and request after end of life; planning upfront to ensure access for life of the system
- There are other titles and statutes in place that protect product availability when national security is at issue
- Dichotomy between what is available commercially and defense purchasing practices.
  - Need to make sustainment decisions at the initial purchase; but DoD policies do not support that approach.
- Commercial OEMs understand the value in last time buys, current policies prevent that in DoD
  - Aerospace industry buys with 10-15 year options; DoD often has systems lasting decades but does not take a long-term acquisition approach

***Moderator Question:*** How can we add to the Trust description to make a clearer definition? Responses from participants included:

- End to end analysis is needed, Program Protection Plans (PPPs) help, but don't go deep enough
- Counterfeit part arena is using trusted supplier in their language but it is not the same as the DMEA Trusted Accredited Supplier; it is crucial we be specific and careful how we use the term
- Trusted could be defined by being able to meet specific requirements no more, no less
- Trusted could be defined by having the confidence to be free of vulnerabilities
- Cyber world in the last 5 years has gone from protection of the castle, to defending your castle, to finally accepting that your castle will be hit, and dealing with it
- Have to assume that nothing is safe, nothing is really secure; we need to develop response plan instead of solely focusing on front-end security

- Trustworthiness of IP is most valued
  - Unless you have the money to design it yourself, you take a risk in buying IP
  - Trust should be a methodology from concept to product
  - Can a system be developed that recognizes when something has been compromised?

## E. Panel "Industry Perspective: Defense Systems Manufacturers"

Dr. Brian Cohen moderated a panel of representatives from defense systems manufacturers and asked them to introduce themselves and provide a brief statement on their view of Trusted Microelectronics.

- Charles Adams, Northrop Grumman
  - Lots of success using Trusted, concerns growing on the future access
- Jessica Denham, Raytheon Company
  - Sees flowing requirements between DMEA and PMO as a challenge
- Dr. Pat Hays, Boeing Defense, Space & Security
  - Sees challenges in low volume supplies
  - Can raise awareness of advanced technologies from commercial sources
- Dr. Mitchell Meinhold, Lockheed Martin
  - Sees ASICs a major player in the plan ahead, especially with increased foreign interests
  - FMS is a big driver for hardware security -- ASICs will be a big part of enabling FMS sales
- Mark Porter, General Dynamics Mission Systems
  - Trusted flow isn't flowing downstream, has not seen Trusted work, almost all work has been done in FPGAs

***Moderator Question:*** What is being flowed down? Have you seen a PPP? Do you have say in how it is written; does it translate to contract language? Panelists' responses:

- Have seen PPPs, helped write, concerned about lost in translation to contract
- Disconnect in portraying the work done in the PPP to the language in the contract
  - Sees value in figuring ways to translate from PPP to contract language

***Moderator Question:*** How can we define requirements as a buyer? Panelists' responses included:

- Consolidating requirement efforts would be ideal, removing outdated or even overlapping orders would reduce confusion
- Would be helpful to help keep the OEM from becoming the middle man and eliminate the back and forth with the customer
- End to end Trust from architecture to product is needed
- The FPGA Trust study shows a good view of the whole supply chain spectrum
- Standardization & policy consistence is needed, also would be great if we could develop technology standards on the industry side
- Creating an OEM working group similar to the TASSG is a great idea

***Moderator Question:*** What controls, as a buyer, do you need? Do you need flexibility? Panelists' responses included:

- Comes back to CPI; how to protect the critical information
- Consolidating requirements on the government side will be helpful
- Communication is key, from end to end – getting the right people in the room to work out requirements in real time
- Weigh performance requirements versus additional demands
- CPI could use more flexibility; 2.5D interposer could be a good solution that would help both performance and integrity
- Commercial world two-way street: Can both benefit and add value but brings the common characteristics of the insiders threat – is using commercial worth the risks?
- Limiting exposure may not be the right answer if we are not worrying about the greatest threats – insider threat appears to be growing

***Moderator Question:*** Are the products offered by the Trusted supplier community enough? Where should they be focusing? Panelists' responses included:

- We could get more creative with how to get Trusted and assured designs
- Can we eliminate 3rd party IP providers by having a Trusted library
- Sustaining today's technology is a concern; how do we roll procurement into future technology

- Reduce the need for chasing after data parts, follow new protocols on risks
- Having one Trusted supplier for a single part is too risky, increase options in the community

***Moderator Question:*** Are there concerns on end use? Panelists' responses included:

- GDSII: the threat is low, but real
- Commercial security is solid (ARM), respected companies have reputable methods for security
- There a need for an Trusted accredited library
- Multi-layer security needs are unfounded
- Nation state level threats are main concern
- Starts with the assumption that the adversary has the design; security by secrecy doesn't work
- PUFs are essential

***Audience Question:*** If DoD stepped out of the way, could industry solve the issues on its own? Panelists' responded:

- No, relationship is important
- Without Trusted suppliers, no chance at all
- No, too many companies would create their own type of qualifications, no way to monitor
- Need a single place to flow down the requirements
- Very robust MPW -- Trusted library -- closed loop through design mask and fab -- would be more cost effective
- Need government investment in foundry and tools

***Audience Question:*** Can we create a Trusted Group on the OEM side similar to the TASSG? Panelists' agreed to explore possibility:

- Would really like to discuss further, involve government, microelectronics and program people

***Audience Comment:*** Commercial groups have existing solutions to security issues. Are the solutions up to government standards? Can the government find a way to leverage the solutions that the commercial industry has solved and offer them to others? Panelists' and participants' comments included:

- Commercial lifespan considerations are vastly different than that of DoD
- Need mutually beneficial environment that correlates to the evolving threat space
- Commercial design groups solve this problem, but are their solutions to the level the government needs?
- Multiple solutions exist -- USG should figure out a way to leverage existing methodologies
- Defense systems do not have same iteration opportunities as in the commercial world

## F. Open Discussion

Mr. Sydney Pope moderated a summary of the topics presented earlier:

***Open Discussion:*** Some key takeaways from today:

- Government involvement is essential to ensure Trust in defense systems
- Without growth in Trust, there will be no GFUS2, and GFUS2 is essential to Trust
- Hybridization regarding Trust could be key
- Consistent understanding of requirements is needed
- Someone has to pay to get this work done
- President's budget is a factor; we need to make investments to protect Trust
- Any other take-aways?
  - Formal methods of technology and tools, creating consistent design definitions (Jasper/Synopsys)
  - What is the best way to pursue the road ahead with OEMs and TASSG?
  - Can a working group be formed to present at next workshop?
  - Not just anti-tamper with Trust, it's ensuring we have access.
  - A Trusted library should be considered

## G. Wrap Up and Next Steps

Dr. Brian Cohen led a discussion about feedback and topics for the next workshop:

- This has been the best workshop yet; valuable feedback from industry, encouraged that the work they are doing is being seen. Understands demand comes from industry, want to keep the ball rolling. Perhaps consider inviting some folks from the Air Force program on secure environments to join the next workshop
- Perhaps talk about what is the plan forward with budget arena
- Brett Hamilton asked to give JFAC update
  - Currently focusing on physical verification, functional verification, and design, EDA Tools and 3rd party IP
- Should we create a task force to explore creating a broader industry Trusted community? Volunteers?
  - Ezra Hall, David Weaver, Pat Hays, Gerry Etzold, Brian Cohen raised hands

# 3. Summary

This sixth workshop in an ongoing series of workshops on Trusted Microelectronics was the best attended in the series and had excellent participation from the audience. The keynote by Mr. David Sobczak gave the participants vital information about GLOBALFOUNDIRES and the newly created GFUS2 for the Trusted Foundry Program. Mr. Sobczak communicated GFUS2's business model and commitment to the military and aerospace markets. He introduced alternative processes to provide leading edge trustable microelectronics in offshore foundries.

The panel discussions and open discussions were interesting and raised a range of concerns about the way forward. The Trusted Accredited Supplier Steering Group panel revealed increases in Trusted business but also raised issues between suppliers and customers with understanding Trust options.

Some of these issues were echoed during the Defense Systems Manufacturers' panel in which OEM representatives discussed the challenges they face being in between the government program offices and the Trusted Suppliers. A suggestion for the Trusted Accredited Supplier Steering Group to develop a users' guide to buying Trusted Microelectronics was heartily embraced by most of the workshop participants.

Many differences in views were presented about how to deal with protecting products that come from global commercial markets. There was further discussion about how the security concerns of a broader community that includes commercial spaces and other nations might be mutually and collaboratively addressed.

In wrapping up the workshop, there was a discussion of the future direction of the Trusted Microelectronics Workshops. Many of the participants felt that forming a working group of government and industry participants to address some of the issues raised would be productive and several people expressed willingness to participate in such an activity. There was a strong desire to continue the dialogue between government, Trusted Suppliers, OEMs, integrators, security experts and contracting experts as the market dynamics and technology progression changes defense microelectronics availability.

# Appendix A:
# Agenda

# TRUSTED MICROELECTRONICS WORKSHOP

8:30am – 8:40am **WELCOME**
Dr. Brian Cohen, *Research Staff Member, Institute for Defense Analyses*

8:40am – 9:30am **TRUSTED MICROELECTRONICS: INTRODUCING GFUS2**
Mr. David Sobczak, *Director, GLOBALFOUNDRIES*

9:30am – 10:00am **DISCUSSION**
Moderator: Mr. Sydney Pope, *Systems Security Engineering Expert, Decisive Analytics Corporation*

10:00am – 10:15am **NETWORKING BREAK**

10:15am – 11:30am **INDUSTRY PERSPECTIVE: DMEA TRUSTED ACCREDITED SUPPLIERS**
MODERATOR
Mr. Sydney Pope, *Systems Security Engineering Expert, Decisive Analytics Corporation*
PANELISTS
- Mr. Wayne DeCarlo, *Vice President, Photronix, Inc.*
- Dr. Brad Ferguson, *Wafer Foundry Services Business Development Manager, Cypress Semiconductor*
- Mr. Scott Jordan, *President, Jazz Semi Trusted Foundry*
- Mr. Stewart Ocheltree, *Program Manager, Space Products & Systems, BAE Systems*
- Mr. Kirk Peterson, *Director of Digital ASICs, Application Products Group, ON Semiconductor*

11:30am – 12:00pm **DISCUSSION**
Moderator: Dr. Brian Cohen, *Research Staff Member, Institute for Defense Analyses*

12:00pm – 1:00pm **LUNCH**

1:00pm – 2:30pm **INDUSTRY PERSPECTIVE: DEFENSE SYSTEMS MANUFACTURERS**
MODERATOR
Dr. Brian Cohen, *Research Staff Member, Institute for Defense Analyses*
PANELISTS
- Mr. Charley Adams, *Director of Programs, Mission Systems, Northrop Grumman Corporation*
- Ms. Jessica Denham, *Principal Systems Engineer, Raytheon Company*
- Dr. Pat Hays, *Chief Engineer, The Boeing Company*
- Dr. Mitch Meinhold, *Senior Research Scientist, Lockheed Martin Corporation*
- Mr. Mark Porter, *Senior Design Assurance Engineering Manager, General Dynamics*

2:30pm – 3:15pm **DISCUSSION**
Moderator: Mr. Sydney Pope, *Systems Security Engineering Expert, Decisive Analytics Corporation*

3:15pm – 3:30pm **WRAP UP AND NEXT STEPS**
Dr. Brian Cohen, *Research Staff Member, Institute for Defense Analyses*

3:30pm **ADJOURN**

### MR. DAVID SOBCZAK, GLOBALFOUNDRIES

Mr. David Sobczak is the Director of Program Management within the Aerospace and Defense business unit of GLOBALFOUNDRIES. In that role, he manages the contractual relationship with the U.S. Government as an accredited Trusted Foundry. He also manages program execution for the Aerospace and Defense business unit, including the Trusted Foundry program as well as direct commercial programs with the defense and intelligence industrial base of customers. Dave was named to this position in July 2015 after the acquisition of the IBM Microelectronics division by GLOBALFOUNDRIES. He served in a similar role with IBM Microelectronics since August 2011, including sales and business development for the division's Aerospace and Defense business. Over his 30-year career, Dave has held a number of sales, development and management roles. In his 18 years with IBM, he started in sales support, managed an ASIC development team focused on the design of re-useable bus interface intellectual property, managed IBM's foundry program management team, and managed the Product and Release Engineering organization for the Microelectronics division. Prior to IBM, he worked in product management with NCR Corporation, sales and applications engineering with LSI Logic Corporation and integrated circuit design with Raytheon. He serves on the board of the Howard Center, Vermont's largest non-profit Health and Human Services agency offering professional crisis and counseling services to children and adults; supportive services to individuals with autism and developmental disabilities; counseling and medical services for those struggling with substance abuse, and intensive interventions for adults with serious and persistent mental health challenges. Dave holds a Bachelor of Science degree in Electrical Engineering from the University of Notre Dame, a Masters of Science degree in Electrical Engineering from Northeastern University and a Masters of Business Administration degree from the Fuqua School of Business at Duke University.

### MR. CHARLES ADAMS, NORTHROP GRUMMAN CORPORATION

Charles Adams is director of Programs for the Northrop Grumman Mission Systems sector's Semiconductor Foundry in Linthicum, Maryland. In this role, his primary focus is to develop discriminating semiconductor technology for DoD products. Prior to his current role, Charley has spent his career in the development of space systems and advanced sensor technologies for multiple customers, and specializes in device level technologies and EO and RF sensor systems. He earned a bachelor's degree in electrical engineering from Georgia Tech and a master's degree in systems engineering from the University of Maryland, Baltimore County. Outside of work, his passion is developing the future generations of scientists and engineers to create innovative solutions for tomorrow. He currently resides in Perry Hall, Maryland with his wife and two young children.

### DR. BRIAN COHEN, INSTITUTE FOR DEFENSE ANALYSES

Dr. Brian Cohen has been a Research Staff Member in the Information Technology and Systems Division of the Institute for Defense Analyses (IDA) for over 25 years. He received his B.S. EE and Mathematics from Carnegie-Mellon University in 1981, an MS ECE, Systems and Control Theory from University of Massachusetts in 1983 and Ph.D. in Engineering Sciences from Thayer School of Engineering, Dartmouth College in 1988. After graduation, he held a research professorship at Dartmouth College until 1991 when he joined IDA. Brian has performed a range of studies at IDA, with a focus on technology and business assessments for national security. Many of these studies have dealt with sensor, electronic and microsystem device technology issues. Recent studies have examined problems with assuring the supply chain for defense systems in the face of increased trends toward offshore sources.

### MR. WAYNE DECARLO, PHOTRONICS, INC.

Wayne DeCarlo is Photronics - Vice President, Military and Aerospace Mainstream Sales Americas and Europe. He has 35+ Years of National and International Mil/Aero Photomask industry experience with prime and secondary contractors, focusing on 65nm and larger design nodes. In addition to overall Sales and Business Development actives in these areas, Wayne is Photronics Corporation Sponsor on the TASSG Team.

### MS. JESSICA DENHAM, RAYTHEON COMPANY

Jessica Denham has been at Raytheon Company for 19 years and has been involved with ASIC/FPGA design and development for the last 15 years. For the last 7 years she has been involved with Trusted development and production and has worked closely with DMEA in the areas of design validation and accredited Trusted suppliers. Jessica earned a bachelor's degree in Engineering Technology and Spanish from Arizona State University and a master's degree in Computer Architecture from Boston University. Outside of work Jessica participates in triathlons and marathons around the country and volunteers her time at the Tucson VA Hospital.

### DR. BRAD FERGUSON, CYPRESS SEMICONDUCTOR

Dr. Bradley Ferguson has over 16 years of experience in the Semiconductor industry both in engineering and business leadership roles. He joined Cypress in 1999 as a lithography Technology Development Engineer, helping to develop and mature processes from 90nm to 0.25um into production. In 2008 he launched a Foundry business unit to provide external customer access to Cypress' world-class production fab. He also led the effort to achieve Trusted Fab accreditation in 2010, which was significant in that it aligns with the fab's long-term vision of foundry manufacturing with a focus on custom Defense markets. Since then Brad has successfully secured Foundry business deals with several defense prime contractors, as well as commercial development customers serving markets that include DNA sequencing and superconductivity-based quantum computation. Brad holds a PhD from the University of Texas at Austin and a BS from the University of Minnesota, both in Chemical Engineering.

### DR. PAT HAYS, THE BOEING COMPANY

Dr. Pat Hays is Chief Engineer at Boeing Secure Computing Solutions where he focuses on the business planning and technology roadmap for Boeing's tamper-resistant secure processors. He joined Boeing in 2013 with its acquisition of CPU Tech. As Vice President at CPU Tech, Pat established the semiconductor business unit and managed the development of the secure processor, acquired by Boeing. Throughout his semiconductor career Pat has specialized in developing new programmable architectures to meet the challenges of new algorithms, especially for telecommunications, video coding and other real-time applications. Pat's career highlights include his work at Bell Labs as principal architect of some of industry's first programmable digital signal processors. He was co-founder and CTO of Lexra and just prior to his current work on secure processors, Pat was Vice President of Engineering at MIPS Technologies. He is a past recipient of the International Solid State Circuits Conference Best Paper Award and his chip designs have shipped hundreds of millions of units. Pat received his undergraduate degree from Harvard and his PhD from MIT, both in Physics.

### MR. SCOTT JORDAN, JAZZ SEMICONDUCTOR TRUSTED FOUNDRY

Scott Jordan is the President of JSTF, a wholly owned subsidiary of Jazz Semiconductor. JSTF is a U.S Department of Defense (DoD) Category 1A and 1B Trusted Supplier, and was formed to meet the US Aerospace & Defense Industry needs for on-shore trusted silicon. He has worked in Design Automation for 30+ years in the CAD departments at RCA, Lucent, Maxim, and Jazz Semiconductor. At Jazz Semiconductor, which is an independent semiconductor wafer foundry for specialty CMOS process technologies optimized for integrated analog and mixed-signal semiconductor chips, he was the Design Support Manager for the Aerospace and Defense Division. He specializes in enabling mmWave and Rad Hard by Design ICs for the A&D customers.

### DR. MITCHELL MEINHOLD, LOCKHEED MARTIN CORPORATION

Dr. Mitchell Meinhold is a senior research scientist at Lockheed Martin Corporation. In this position, he has a multifaceted role in which he leads research in hardware security, nano-electronics development and advanced material applications. He is a site-lead running research operations at a Lockheed Martin nano-fabrication facility located in Billerica, MA which is part of the Advanced Technology Center, Space Systems Company (headquartered in Palo Alto). Mitch works with other subject matter experts across the four major business areas of the company addressing the challenges of hardware security and trusted microelectronics. He also works with leaders in the corporation to stay abreast

of policy and leads a Fellows Action Team (FACT) on secure and trusted hardware which meets periodically to discuss this important topic. He also presented the corporate strategy for trusted microelectronics acquisition at a recent LM Technology Symposium. Prior to his 7-year career at Lockheed Martin, he developed advanced non-volatile memory at Nantero, a Woburn MA based startup company founded in 2003. Mitch received his PhD and MS from MIT in 2003 and 1996 respectively and a BS in EE and BS in Engineering Physics from Lehigh University in 1994.

### MR. STEWART OCHELTREE, BAE SYSTEMS

Stewart Ocheltree a program manager in Space Products and Systems at BAE Systems, Manassas, focused on new product and technology programs. He has over thirty years of experience in both commercial and defense microelectronics. Prior to joining BAE Systems, Stewart was the fab engineering manager at Micron's Manassas DRAM and NAND Flash fab. He spent 15 years at IBM Microelectronics and was part of the management team that established the joint venture fab with Toshiba in Manassas. He holds a B.S. in Electrical Engineering from Virginia Tech.

### MR. KIRK PETERSON, ON SEMICONDUCTOR

Kirk Peterson manages the ON Semiconductor digital ASIC business unit focusing on military and aerospace applications. He has more than 30 years of experience in business management, marketing, and engineering. He began his career at Analog Devices and Intel before joining ON Semiconductor. Kirk graduated from Idaho State University with a BS in Mathematics with Computer Science emphasis. He attained the Project Management Institute's Project Management Professional (PMP) status in 2005 and is a certified black belt in Lean Six Sigma.

### MR. SYDNEY POPE, DECISIVE ANALYTICS CORPORATION

Mr. Sydney Pope joined Decisive Analytics Corporation in 2013 as a support contractor to the Office of the Deputy Assistant Secretary of Defense for Systems Engineering. He is the Department's lead systems security engineering expert on the preservation of trusted, reliable and sustainable electronic hardware. Among his duties, he assists major defense acquisition programs in developing protection plans for managing supply chain risks from malicious acts and the development of the Department's assured microelectronics policy. Prior to his current assignment, Syd was a member of Office of the Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy as a business and technical expert in industrial affairs. For nine years he was the Department's lead industry analyst for weapon systems, including electronic hardware, soldier equipment, and ground vehicles. He managed the Department's use of Defense Production Act Title I authority including the Defense Priorities and Allocation System and the establishment of Security of Supply arrangements with allied nations. He also was the industrial policy lead for domestic preference legislations such as the Specialty Metals Provision and the Berry Amendment. Among his academic achievements, Syd has a bachelor's degree in industrial engineering from the University of Buffalo, a master's in management from Salve Regina University, a diploma in International Security and Strategic Studies from the U.S. Naval War College, and is a Certified Professional Contracts Manager by the National Contract Management Association.

### MR. MARK PORTER, GENERAL DYNAMICS

Mark Porter is a Senior Design Assurance Engineering Manager at General Dynamics Mission Systems in Scottsdale, Arizona. He is responsible for all Specialty Engineering activities supporting Space and Intelligence Systems Programs. He has over 30 years of experience managing and motivating technical personnel at multiple sites throughout the country. He personally has detailed experience working System and Specialty Engineering on Satellite Systems, Launch Vehicles, Upper Stage Vehicles, and Military Airplanes. His support has included everything from piece part and material procurements through board and box assembly, subcontracted box and system procurements, failure analysis, reliability analyses, contamination control, and launch site logistics planning and support. He is the chairman emeritus for the SAE SSTC G12 Committee and was responsible for arranging, planning, and chairing 3 meetings per year involving DoD, NASA, JAXA, ESA, DLA, The Aerospace Corporation, OEM industry, and the piece part manufacturing industry.

# Appendix B: Introducing GLOBALFOUNDRIES U.S. 2, David Sobczak

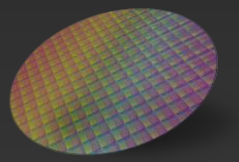
# Introducing GLOBALFOUNDRIES U.S. 2

*- David Sobczak, Trusted Production Officer*

GLOBALFOUNDRIES®

# Agenda

Company Overview



Future of Trusted Semiconductors

# The GLOBALFOUNDRIES Story

## Creating an industry leader

- AMD spins out fab operations
- Mubadala (ATIC) acquires majority stake
- GLOBALFOUNDRIES created
- Construction begins on New York fab

Acquires Chartered Semiconductor

- New York fab delivers initial silicon first time right
- 100% ownership by Mubadala
- Dresden fab ships 250,000th 32nm HKMG wafer

Launches 14nm FinFET technology

- Sanjay Jha joins as CEO
- Collaborates with Samsung on global 14nm manufacturing
  - Acquires IBM Microelectronics business
  - GFUS2 formed
  - Launches 22nm FD-SOI technology
  - Launches 14nm FinFET ASIC offering

2009 2010 2011 2012 2013 2014 2015

Largest privately held semiconductor company

~8X capacity increase since 2009

# GLOBALFOUNDRIES Company Highlights

## REVENUE

~6B*

2nd Largest Foundry

## MORE THAN

25,000
Patents & Applications

250
Customers

18,000
Employees

## FAB LOCATIONS


Trusted Foundry

## FAB CAPACITY

300mm
200K Wafers/Mo

200mm
133K Wafers/Mo

*Based upon analysts' estimates

# Global Manufacturing Capacity: ~7M Wafers/Yr*

| East Fishkill, New York (Fab 10) | Malta, New York (Fab 8) | Burlington, Vermont (Fab 9) | Dresden, Germany (Fab 1) | Singapore (Fabs 2-7) |
|---|---|---|---|---|
|  |  |  |  |  |
| **TECHNOLOGY** | | | | |
| 90nm – 32nm | ≤ 14nm | 350nm – 90nm | 28nm – 22nm | 180nm – 40nm |
| **CAPACITY IN WAFERS/MONTH** | | | | |
| 14,000 (300mm) | Up to 60,000 (300mm) | 40,000 (200mm) | 60,000 (300mm) | 68,000 (300mm)<br>93,000 (200mm) |

*200mm Equivalents

# 2015 Semiconductor Ranking Including Foundries

| Rank | Company | Region | 2015F Sales |
|---|---|---|---|
| 1 | Intel | U.S. | 50,305 |
| 2 | Samsung | S. Korea | 41,606 |
| 3 | TSMC | Taiwan | 26,562 |
| 4 | SK Hynix | S. Korea | 16,917 |
| 5 | Qualcomm | U.S. | 15,632 |
| 6 | Micron | U.S. | 14,816 |
| 7 | TI | U.S. | 12,112 |
| 8 | Toshiba | Japan | 9,734 |
| 9 | Broadcom | U.S. | 8,421 |
| 10 | Avago | Singapore | 6,961 |

| Rank | Company | Region | 2015F Sales |
|---|---|---|---|
| 11 | Infineon | Europe | 6,898 |
| 12 | ST | Europe | 6,840 |
| 13 | MediaTek | Taiwan | 6,504 |
| 14 | Sony | Japan | 5,885 |
| 15 | NXP | Europe | 5,790 |
| 16 | Renesas | Japan | 5,664 |
| 17 | GLOBALFOUNDRIES | U.S. | 4,990 |
| 18 | Nvidia | U.S. | 4,628 |
| 19 | UMC | Taiwan | 4,474 |
| 20 | Freescale | U.S. | 4,410 |

**Source**
**IC Insights, McClean Report, September 2015 Update, Fig. 1**

# Key Markets Driving Growth

## CONSUMER, WIRELESS, MOBILE COMPUTING

- Cellular/WiFi Connectivity
- Smartphones

- Tablets
- Portable

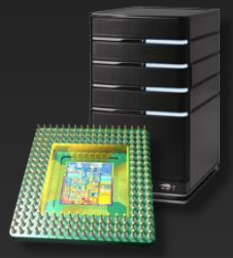
## WIRED & WIRELESS INFRASTRUCTURE

- Basestations
- Routers/Switches

- Digital TV
- Set-top Boxes


## HIGH PERFORMANCE COMPUTING

- Microprocessors
- Networking
- Servers/Storage
- Supercomputers

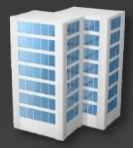


Graphics

# Key Expansion Markets

## INTERNET OF THINGS (IoT)


Smart Cards

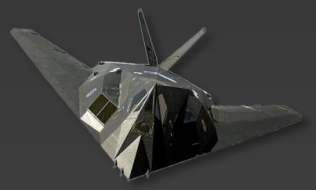


Building Management

Household Appliances

Wearables

## AEROSPACE AND DEFENSE



## INDUSTRIAL


Consumer Medical

Factory Automation

## AUTOMOTIVE

Infotainment

Powertrain Control

Safety Systems

Body Control

# Business Unit Structure

## CMOS Platforms BU

Broad technology portfolio across Leading-Edge & Mainstream nodes

## RF BU

Accelerating RF leadership and manufacturing scale

Differentiated RF portfolio solutions such as RF SOI, RF CMOS, and SiGe

## ASIC BU

Richest portfolio of best-in-class IP for wired, wireless infrastructure applications in the foundry industry

## Aerospace & Defense BU

Leveraging offerings across all BUs to provide solutions for Trusted, Aerospace, and Defense applications, spanning both government and commercial markets

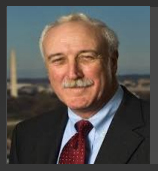
# GLOBALFOUNDRIES U.S. 2 Operating Structure

**GLOBALFOUNDRIES U.S. 2 LLC**
**Board of Directors**

**Kenneth Krieg**
Outside Director, Government Security Committee Chair
Former Undersecretary of Defense, AT&L

**James Doyle**
Chair, Board of Directors
Officer Director
Government Security Committee
SVP & General Mgr Fab Management

**Lou Lupin**
Inside Director
SVP and Chief Legal Officer



**Sean O'Keefe**
Outside Director
Government Security Committee
Former Secretary of the Navy and NASA Administrator

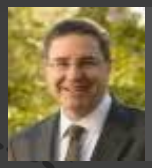
**John Bucher**
Officer Director
Government Security Committee
Senior Vice President, Strategy

**Dr. John Goldsberry**
Inside Director
Chief Financial Officer

**Tony Tether**
Outside Director
Government Security Committee
Former DARPA Director

**Anthony Yu**
Officer Director
Government Security Committee
Sr. Director, A&D Business Unit

**Mike Cadigan**
Officer Director
SVP, Product Management Group



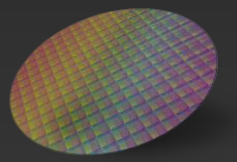
**Karmi Leiman**
Board Secretary
Technology Control Officer
Sr. Director, Import/Export

**David Sobczak**
Trusted Production Officer
Director, Program Management

**Carmine Mele**
Corporate Facility Security Officer
Director, Government Relations

# Agenda

Company Overview



Future of Trusted Semiconductors

# GLOBALFOUNDRIES Trusted Technology Portfolio

## *- Fabs 9 and 10 through the Trusted Access Program Office*

| Node | ASIC | Digital Foundry | | | RF Foundry | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | SOI CMOS | CMOS | Low-Power CMOS | SiGe PA | SiGe HP | RF SOI | RF CMOS | High-Voltage CMOS |
| 32nm | Cu-32 | 32SOI | | | | | | | |
| 45nm | Cu-45 | 12S0 | | | | | | | |
| 65nm | | | 10SF | 10LP | | | | 10RFe | |
| 90nm | | | 9SF | 9LP | | 9HP◊ | | 9RF | |
| 130nm | | | 8SFG | | | 8XP<br>8HP<br>8WL | | 8RF | |
| 180nm | | | | | | 7WL | 7SW SOI*<br>7RF SOI | 7RF<br>7TG | 7HV |
| 250nm | | | 6SF | | | 6WL | | 6RF | |
| 350nm | | | | | 1KW5PAe*<br>5PAe | 5HPE* | | | |

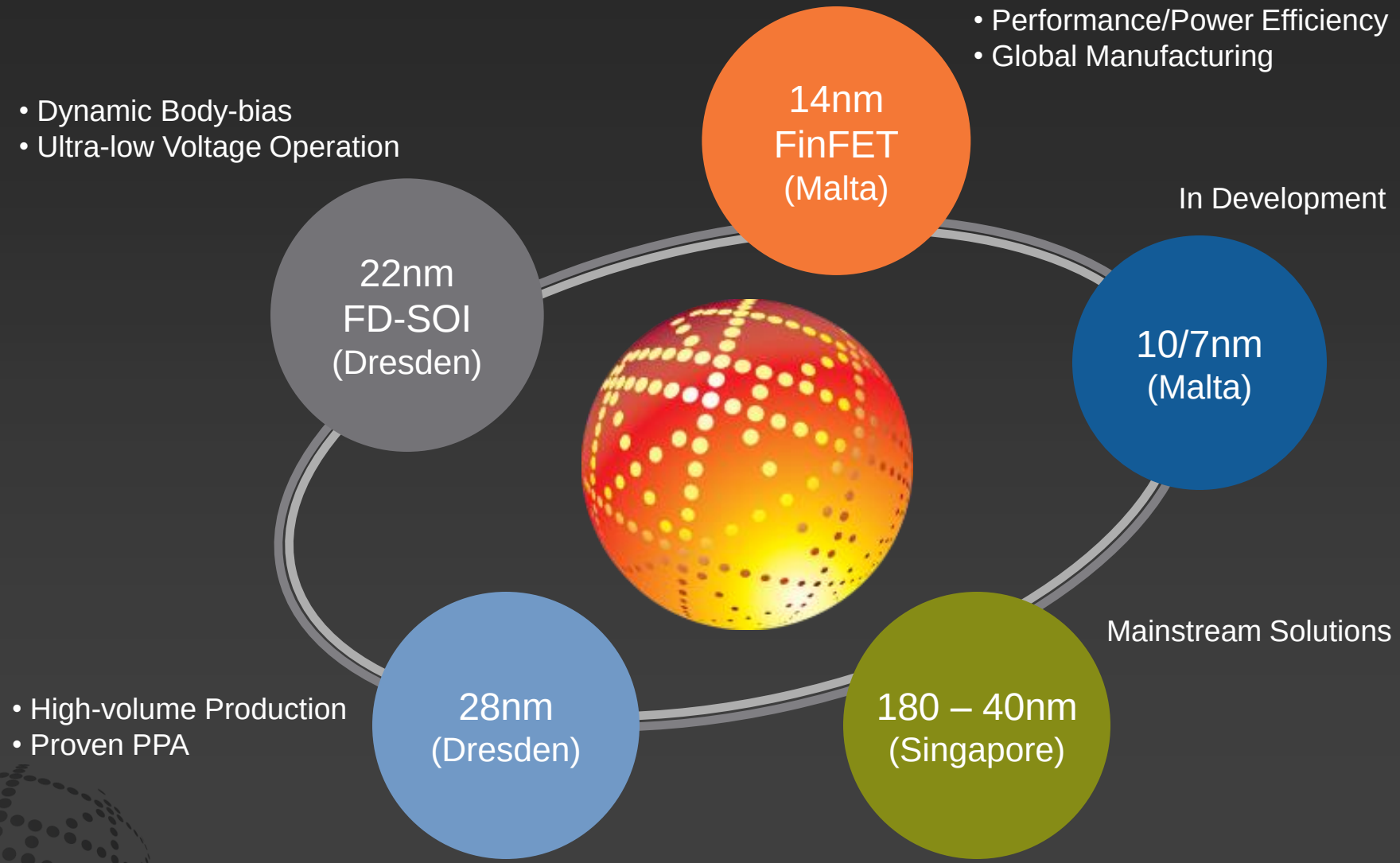
◊ In development
* Potentially available by individual program quote

# GLOBALFOUNDRIES Trusted Capabilities

| | *Commercial* | *ITAR* | *Trusted* |
|---|---|---|---|
| *Design Services* | ✓ | ✓ | ✓ |
| *Data Preparation and Release* | ✓ | ✓ | ✓ |
| *Mask Build* | ✓ | ✓ | ✓ |
| *Wafer Manufacturing – Fab 9 (Burlington, VT)* | ✓ | ✓ | ✓ |
| *Wafer Manufacturing – Fab 10 (East Fishkill, NY)* | ✓ | ✓ | ✓ |
| *Wafer Test* | ✓ | ✓ | ✓ |
| *Post-Wafer Manufacturing* | ✓ | ✓ | ✓ |
| *Packaging** | ✓ | ✓ | ✓ |
| *Module Test* | ✓ | ✓ | ✓ |
| *Pack and Ship* | ✓ | ✓ | ✓ |

** Sub-contracted*

# Broad Range of Optimized Process Platforms



# New Trust Model for Advanced Nodes
## *- "Hybrid" Trust?*

| | IP / Kits | Release / Dataprep | Mask Fab | Wafer Fab | Post-Fab | Test | Packaging |
|---|---|---|---|---|---|---|---|
| ***Trusted*** | | | | | | | |
| ***Hybrid*** | | | | | | | |
| ***ITAR*** | | | | | | | |
| ***Commercial*** | | | | | | | |

| | |
|---|---|
| ***Commercial*** | - Standard commercial offering protection of data/assets |
| ***ITAR*** | - Work performed in the US by US Persons<br>- Physical access control to hardware<br>- Logical access controls to US based commercial IT |
| ***Trusted*** | - Work performed in cleared facilities<br>- 24/7/365 cleared security team oversight<br>- IT in dedicated air gapped cleared facility |

# “Split Fab” to enable “Trusted” use of off-shore fabs?


## Considerations:

- ROI and associated opportunity cost – what is the market demand?
- Enablement requirements (design manuals, design kits, EDA flows, etc.)?
- Technology qualification requirements (temp ranges, reliability, warranties, etc.)?
- IP qualification requirements (base libraries, memory compilers, hard IP, etc.)?
- Sufficient volume for yield learning and on-going offering viability?

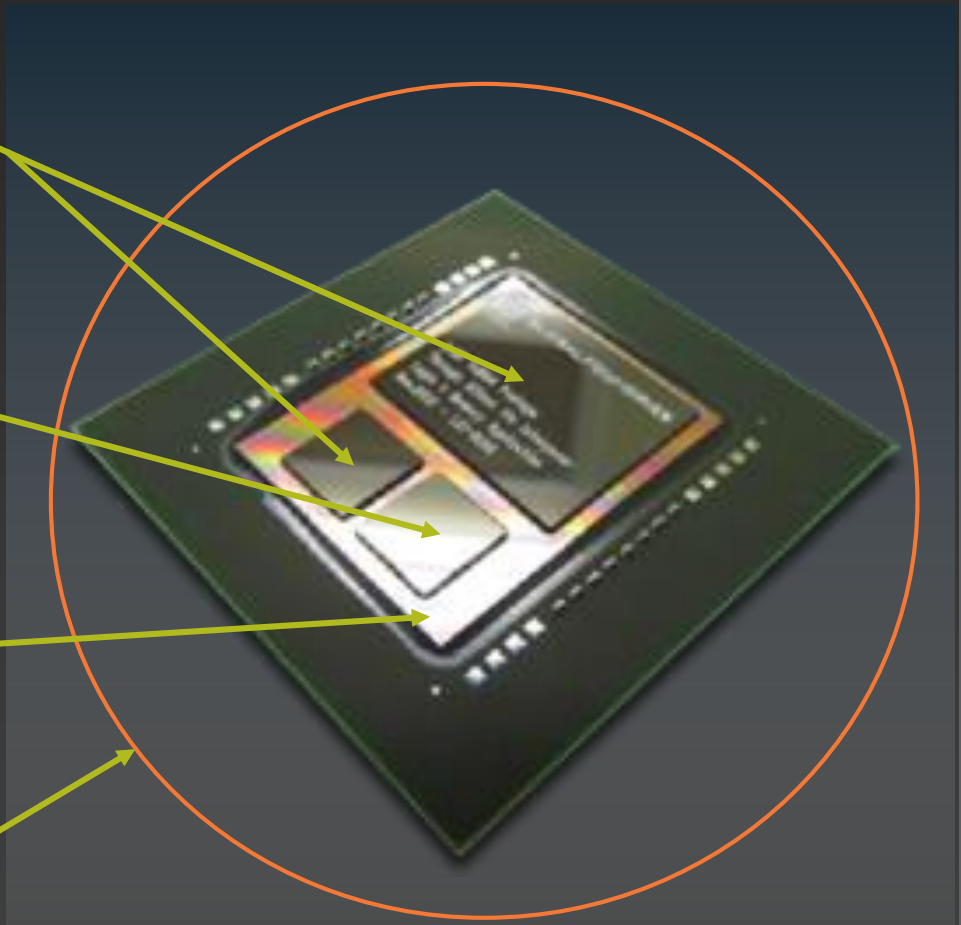
# 2.5D TSV Si Interposer: Architected for Trust

**Advanced Technology Die (Non-Trusted)**

**Specialized Die (Trusted)**

**Interposer (Non-Trusted)**

**Assembly and Test (Trusted)**



# Summary

- GLOBALFOUNDRIES is committed to the Trusted Foundry program
- Fabs 9 and 10 maintained un-interrupted Trusted accreditation through the transition to GLOBALFOUNDRIES
- GLOBALFOUNDRIES continues to invest in Fabs 9 and 10 through both infrastructure and technology investments
- The Aerospace and Defense Business Unit is strategically driving for significant growth in the next 5-10 years
- We are supporting an assessment of our advanced node, highly automated, Fab 8 facility in Malta, NY to determine what it would take to run product requiring higher levels of export control and security for your critical government programs
- Announcing the return of the annual Trusted Foundry Advanced Technology Training in Burlington, VT – 3-4 May 2016
  - **https://www.eventbrite.com/e/2016-trusted-foundry-advanced-technology-training-tickets-19619474376**

***See you at GOMACTech 2016! – Booth 407***

# Thank you

# Appendix C:
# Attendees

Charles Adams, Northrop Grumman

John Adams, The Aerospace Corporation

Brett Attaway, Synopsys, Inc.

Anita Balachandra, TechVision21

Stephen Basile, The Eisenhower School-National Defense Univ.

Brad Botwin, Bureau of Industry and Security, Department of Commerce

Dean Brenner, Honeywell International

Shane Brockway

Kathy Brown, Covington & Burling, LLP

Theodore Bujewski, OSD/AT&L/Manufacturing and Industrial Policy

Mary Caruso, Honeywell - Kansas City Plant

Patrick Cheetham, Potomac Institute for Policy Studies

Robert Ciccariello, Byte Cubed

Brian Cohen, Institute for Defense Analyses

Douglas Cummings, The Aerospace Corporation

David Davis, USAF/SMC

Wayne DeCarlo, Photronics, Inc.

Jessica Denham, Raytheon Company

Emmanuel Digman, DoD-NSA

Michael Dixon, The Eisenhower School-National Defense Univ.

StevenEdwards, Curtiss- Wright Controls Embedded Computing

Gerald Etzold, Etzold Technology Consulting

Bradley Ferguson, Cypress Semiconductor Corporation

Matthew French, USC-Information Sciences Institute

Michael Fritze, Potomac Institute for Policy Studies

Michelle Geitzenauer, Rockwell Collins

Jim Gobes, Intrinsix

Jason Gorey, Six O'clock Ops., LLC

David Gottfried, Smart System Technology and Commercialization Center (STC)

Ezra Hall, GlobalFoundries

John HallmanJr., MacAulay Brown, Inc.

Brett Hamilton, Naval Surface Warfare Center, Crane Division

John Hamma, Novati Technologies

Idriys Harris, The Aerospace Corporation

Russell Haymes, Battelle

W. Patrick Hays, Boeing Company

Craig Herndon, Naval Surface Warfare Center-Crane Division

Joseph Holt

Alan Howard, Wyle

Michael Johnson, Sandia National Laboratories

Scott Jordan, Jazz Semiconductor Trusted Foundry

Efthimios Katsapis, PREVISE, LLC.

Harry Kellzi, Teledyne Microelectronic Technologies

Christopher Kirshak, The Aerospace Corporation

Thomas Knight, Northrop Grumman Corporation

Kenneth Lebo, Van Dyke Technology Group

Henry Livingston, BAE Systems

Jon Lunglhofer, Northrop Grumman Electronic Systems

Jeff Magee, GlobalFoundries

Marie Mak, U.S. Government Accountability Office

Daniel Marrujo, DMEA

Michael Martin, LitCon Group, LLC

Mona Massuda, National Security Agency

Erika Maynard, Bureau of Industry and Security, Department of Commerce

Michael McGrath, McGrath Analytics, LLC

Michael Mehlberg, Cryptography Research, Inc.

Mitchell Meinhold, Lockheed Martin Advanced Materials & Nanosystems

Janice Meraglia, Applied DNA Sciences

David Meshel, The Aerospace Corporation

Eric Miller, The Boeing Company

Jeffrey Miller, Northrop Grumman Electronic Systems

Joseph Misanin, Misanin Technology Ventures, LLC.

John Monk Jr., Northrop Grumman

Michele Moss, Booz Allen Hamilton

James Murray Jr.

Mike Newman, Aeroflex Incorporated

Stewart Ocheltree, BAE Systems

Catherine Ortiz, Defined Business Solutions

Doug Palmer, Booz Allen Hamilton

Kirk Peterson, ON Semiconductor

William Phillips, Northrop Grumman Corporation

Sydney Pope, Decisive Analytics Corporation

Jimmy Poplin, Defined Business Solutions

Mark Porter, General Dynamics Mission Systems

Nathan Price, The Aerospace Corporation

Paul Quirk, National Secure Manufacturing Center

Daniel Radack, Institute for Defense Analyses

Robert Reams, SEDD Directorate

Kirk Reynolds, Rockwell Collins

Marcia Sawhney, National Security Agency

Timothy Scott, Novati Technologies

Frederick Sexton, Sandia National Laboratories

Raymond Shanahan, DASD(SE)

Vashisht Sharma, Institute for Defense Analyses

Thomas Sharpe, SMT Corp

Colin Smolinsky, Jacques & Associates, Inc.

David Sobczak, Global Foundaries

Paul Syers, Potomac Institute for Policy Studies

Michael Tierney, Jacques & Associates, Inc.

Samantha Ulrich, Northrop Grumman

David Weaver, SRI International Sarnoff

John Weaver, Tectonic Labs, LLC.

Kenneth Wetzel Jr., Strategic Marketing Innovations

Melinda Woods, Department of Defense-OSD

Candice Wright, U.S. Government Accountability Office

Edwin Yarbrough, Honeywell International