NDIA Electronics Division Kick-off

January 18, 2018

Agenda

Time		
0830-0845	Welcome	Lockheed Martin
0845-0910	NDIA CEO Comments	General Carlisle
0910-0920	Officers Introduction	Dave Chesebrough
0920-0945	NDIA Electronics Division Vision	Officers
945-1000	Break	
1000-1030	Key Note Speaker	Ms. Kristen Baldwin
1030-1140	Government Panel: “Key Challenges the USG Faces with respect to Electronics”	Panelists: Government Liaison Committee
1140-1240	Lunch	
1240-1330	Industry Panel #1: “Key Challenges Industry Faces with respect to Electronics”	Panelists: Industry Representatives
1330-1420	Industry Panel #2: “Key Challenges Industry Faces with respect to Electronics”	Panelists: Industry Representatives
1420-1435	Break	
1435-1515	Committee Topics	Officers
1515-1530	Activities and Schedule	Officers
1530-1545	Call for Volunteers	Officers
1545-1600	Actions and Wrap Up	Officers

Lockheed Martin

WELCOME

General Carlisle

NDIA CEO COMMENTS

Dave Chesebrough

OFFICERS INTRODUCTIONS

Executive Committee

Chairman

Kelly Jill Hennig, Manager of Strategic Planning, Northrop Grumman Corporation

Secretary

Anita Balachandra, CEO, TechVision21

Officers-at-Large

Ezra Hall, Director, Aerospace & Defense Programs, GLOBALFOUNDRIES

Kathleen N. “Taffy” Kingscott, Vice President, Strategic Partnerships, IBM Research

Grant Meyer, Director, Federal Strategy and Business Development, SRI International

Kelly Hennig

ELECTRONICS DIVISION VISION

The Electronics Division History

- The Electronics Division originates from NDIA hosted workshops that occurred between 2013 and 2017.
- Workshops were organized twice a year and addressed a range of topics central to Trusted and Assured microelectronics sources for defense systems.
- At the sixth workshop, a suggestion led to the formation of the Trusted Microelectronics Joint Working Group (TM JWG) in May 2016.
- The TM JWG completed four white papers in July 2017. This work formed the basis for creating the Division that is formally being kicked-off today

Success of Trusted Microelectronics Joint Working Group provides robust foundation for new Electronics Division.

Mission

- Our Mission:
  - To lead the evaluation of current and future challenges, and to develop proposed solutions to address such, for the U.S. Government and industry to access and provide trusted and assured electronics.
- We do this by:
  - Providing a framework for the legal and ethical exchange of information
  - Providing a forum for the interchange of views between the defense industry, commercial industry, universities, research centers, standards bodies, government and military representatives, on trusted and assured technology spanning advanced R&D and design to manufacturing to deployment of systems that target defense and national security end use applications.
- Broadened our scope from microelectronics to electronics:
  - design, manufacturing, packaging, assembly, test, and support

Mission includes all electronics and the industrial base needed to supply electronics for defense and security.

General Objective

- Establish and facilitate a collaborative industry/academia/ government effort to address critical issues for U.S. access to technology to produce trusted and assured components for electronic systems for defense, national security, and critical commercial applications
- Examine the use of
  - trust and assurance enabling technologies where appropriate
  - product integrity and mission assurance
  - government guidance, policy and processes
  - issues facing industry including technical, business, and legal challenges
- Coordinate our objectives with other NDIA divisions, to leverage optimally the core competencies in other divisions according to their subject matter expertise

Collaboration, feedback, and dialogue are essential to fully address critical challenges.

Initial Specific Objectives

1. Facilitate focused engagement between industry and government to collaborate on policy, strategy, and implementation matters relating to electronics
2. Mutually address matters with direct and indirect impacts to electronics
3. Provide education opportunities for all parties through outreach to industry, including non-defense industry, and government
4. Foster collaboration between government and industry to simultaneously achieve confidentiality and integrity goals of trust and assurance by increasing availability from the electronics supplier base
5. Navigate the various degrees of protection, assurance, and or trust required by the government for various classes of electronic systems and components thereto;

Initial Specific Objectives

6. Act as a bridge between commercial electronics suppliers, the government, and Defense Industrial Base, by fostering an environment for mutually sharing insights, strategic thinking, government policy considerations, the needs of government and the national security concerns of the Defense Industrial Base, and the broader needs of commercial electronics industry
7. Collaborate on larger issues
8. Identify investment areas for future acquisition needs
9. Host or support events focused on specific goals or topics
10. Optimally leverage interaction with other NDIA divisions in furtherance of this divisions goals, and to support other NDIA divisions in electronics related matters in support of the other NDIA divisions' goals.
11. Optimally align the timing of this division's activities and work products for usefulness within the context of annual government policy, procurement, and funding cycles.

Participation

- Representatives of Regular Corporate Members of the NDIA Association
- Government Liaison Representatives
- Non-government Individual Members who from experience or special training may contribute to the functions of The Divisions
- Selected experts drawn from the academic, engineering, commercial and industrial communities regardless of NDIA membership status

Membership is open to all who have an interest in electronics for national defense and security.

Organization

- The Division consists of the following:
  - Executive Committee
  - Government Liaison Committee
  - Standing and ad-hoc sub-committees
  - Working groups

Volunteers are needed on many sub-committees and working groups to accomplish our objectives.

Ms. Kristen Baldwin

KEYNOTE SPEAKER

Panelists: David Pentrack, Jeremy Muldavin, Robert Irie & Brad Botwin
Moderator: Ezra Hall

GOVERNMENT LIAISON COMMITTEE PANEL

Panelists: David Isaacs, Scott Bukofsky, Joe Jarzombek & Ken Hansen

Moderator: Taffy Kingscott

INDUSTRY PANEL #1

Panelists: Scott Anderson, Stewart Ocheltree, & Doug Medcalf

Moderator: Grant Meyer

INDUSTRY PANEL #2

Anita Balachandra

SUBCOMMITTEE TOPICS

Subcommittee Topics

1. Trust & Assurance
2. Defense Electronics Industrial Base
3. Strategy and Policy

Trust & Assurance Subcommittee

Mission: Facilitate evolution of Trust and Assurance

- Form/maintain Industry/Government stakeholder team comprised of:
  - Experts spanning pertinent knowledge domains
  - Key decision makers and influencers in Government
  - Representatives from supplier base spanning commercial to Trusted
- Foster an innovative environment for bringing great ideas to action
- Enable interactive development of Trust and Assurance constructs
  - Evaluate and leverage commercial best practices
  - Collaborate to develop / evolve security approaches that mutually satisfy Government needs while aligning with commercial industry capabilities
- Support Government development / refinement of strategy and policy
  - Facilitate forums for development / review / feedback
  - Call industry meetings to enable efficient feedback from industry
- Continue development of integrated Trust and Assurance risk model
- Facilitate involvement of academic and non-profit orgs as appropriate

KEY – Foster government industry co-development of Trust and Assurance approaches and related strategies, policies, and new initiatives

Trust & Assurance Subcommittee – Model Development

Model Goal: Enable efficient tool to address program specific security needs by modeling countermeasures applied to commercial and trusted processes

- **Concept**
  - Catalog Trusted and non-Trusted supplier risk profiles, and countermeasure risk reductions
  - Enable assessment of supply chain risk at program level, across the Trusted and/or Commercial suppliers selected for a given program
  - Facilitate selection of necessary countermeasures to satisfy program security requirements
  - Determine resulting risk profile for input as evidence to program protection plan
- **Goals**
  - Enable capture of quantitative risk assessments for comprehensive catalog of countermeasures and suppliers
  - Provide an analytical casual framework for risk analysis
  - Enable answering key program questions and challenges relative to risk:
  - Are my mitigations "right-sized"?
    - Do I have enough protection to meet my requirements?
    - Are all of the countermeasures I'm employing necessary to meet requirements?
  - Am I utilizing commercial IP, manufacturing and processes appropriately?
    - Does use of unmitigated COTS meet my security needs?
    - How many and which countermeasures need to be layered on top of existing commercial IP or practices?
    - Am I properly accounting for the strength of existing commercial countermeasures?
  - Is the benefit of a specific countermeasure worth the cost (performance, schedule dollars)?

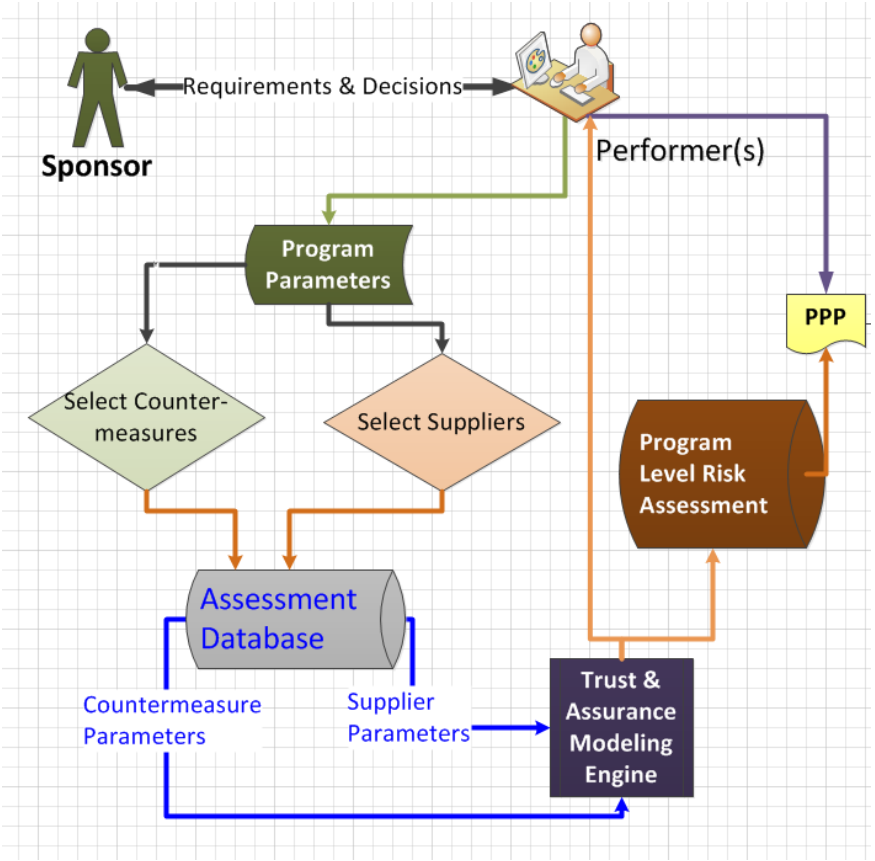
KEY: Industry – Government collaboration is critical to developing operable means of achieving security goals

Trust and Assurance Modeling

Tools are needed to enable countermeasure / supplier risk assessment

Effort status

- Concept developed in 2017 under NDIA Joint Working Group 2
- Stakeholders engaged, sub teams formed
  1. Program requirements
  2. Model development
  3. Countermeasure assessment
  4. Supplier assessment
- Current focus items:
  - Risk assessment methodologies
  - Catalog structure
  - Risk modeling engine
- Additional members welcome



Key: Efficient model must be developed in collaboration with all users of the tool to enable a solution.

Defense Electronics Industrial Base Subcommittee

Mission: Raise awareness of the vulnerabilities in the entire defense industrial base for electronics with respect to trust and assurance.

- Broadens our previous look at microelectronics end to end flow, and includes packaging, assembly, surface mount components, boards, test, commercial of the shelf, and reliability screening
- Includes an examination of smaller commercial suppliers and smaller defense-specific suppliers
- Identifies vulnerabilities and threats with respect to these suppliers for assurance and trust.

Understand entire strength of our industrial base for all electronics needed for national security and defense.

Strategy and Policy Subcommittee

Mission: Develop stakeholder input for U.S. government agencies

- Represent industry viewpoint, including diverse perspectives from different elements in the supply chain
- Highlight factors for consideration in strategies under development
- Articulate the potential impact of policies and programs on commercial partners, defense industrial companies, academic and non-profit orgs
- Identify issues on the horizon for joint consideration with USG partners

KEY - Provide coordinated input to the government in Formulation of strategies, policies and new initiatives.

Strategy and Policy Subcommittee

Projected Efforts:

- **Executive Order 13806**: Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency
  - NDIA Workshop - December 15 – Issue findings follow (Thanks, SIA!)
- **Executive Order 13800**: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- **National Security Strategy**: Announced Dec 2017
- **National Semiconductor Strategy (TBD, 2017 NDAA Sec. 231)**
  - Trusted Microelectronics Joint Working Group white papers provided formal input in 2017.

Sample Issues Identified Executive Order 13806

- **Contracting issues:**
  - Mismatch in timescales – 70 days to contract in private industry, 700 average with government
  - Increase Other Transaction Authority (OTA) for R&D and prototyping
  - Federal Acquisition Regulations (FAR) and Defense FAR (DFAR) often too onerous for commercial companies
- **Preventing counterfeits, malicious parts in supply chain:**
  - Fundamental mismatch between lifetimes of SOA semiconductor components (< 10 years) and DOD systems (decades)
  - Reform procurement policy, for example, allow contractors to do life-time buys for discontinued components needed in legacy systems
  - Build in full, realistic lifecycle costs in procurements
  - Consider commercial avionics and automotive practices as model for long-term relationships with component suppliers in initial contracting
    - Commercial avionics companies require potential component manufacturers to commit to produce parts for lifetime of the system

Sample Issues, continued

- **Global supply chains: Fundamental issue - DOD is 1% of semiconductor market**
  - IP is critical . Focus on design IP at the FEOL and verify fab output on BEOL
  - Encourage large U.S. industries, companies (automotive, Google, Apple, etc.) to use more domestic supply chains
  - Incentivize fabless companies to use U.S. foundries and foundry investment in U.S.
  - Develop common parts lists across DOD to aggregate buying
- **Developing the domestic supply chains of tomorrow:**
  - Invest in new technologies (AI systems, neuromorphic computing, quantum computing) to build domestic supply chains around these emerging technologies
  - Develop next genation R&D consortia & collaborate between component designers, manufacturers, and systems co's to innovate across all Technology Readiness Levels (TRLs)
- **Address export control policies, which can impede collaboration with USG**
  - Existing processes ID'd as rad hard are subject to export control; so companies may simply avoid characterization, thus unable to provide defense capability
  - Examine/reduce export controls on globally available technologies
- **Use broader commercial markets to drive demand for trusted microelectronics**
  - Build awareness of cyber vulnerabilities within larger commercial markets like automotive and infrastructure
  - Work with NIST and others to develop standards for trusted components

National Security Strategy

- **Announced in December**
  - Effective implementation will require USG/industry/academia collaboration
- **Examples:**
  - Improve critical infrastructure risk in national security, energy & power, banking & finance, health & safety, communications, transportation
  - Modernizing federal IT
  - Build culture of preparedness
  - Lead in research, technology, invention and innovation
    - Improve USG understanding of global S&T trends which affect USG strategies
    - Improve collaboration with industry and academia and technical talent recruiting
    - Align USG and private sector R&D resources toward national security apps
    - Improve risk taking and rapid fielding of USG R&D
  - USG to increase understanding of global trade challenges
  - USG to increase protections of IP & technical knowledge by foreign competitors

Strategy and Policy Subcommittee

Process: Maximize participation and minimize the time commitment.

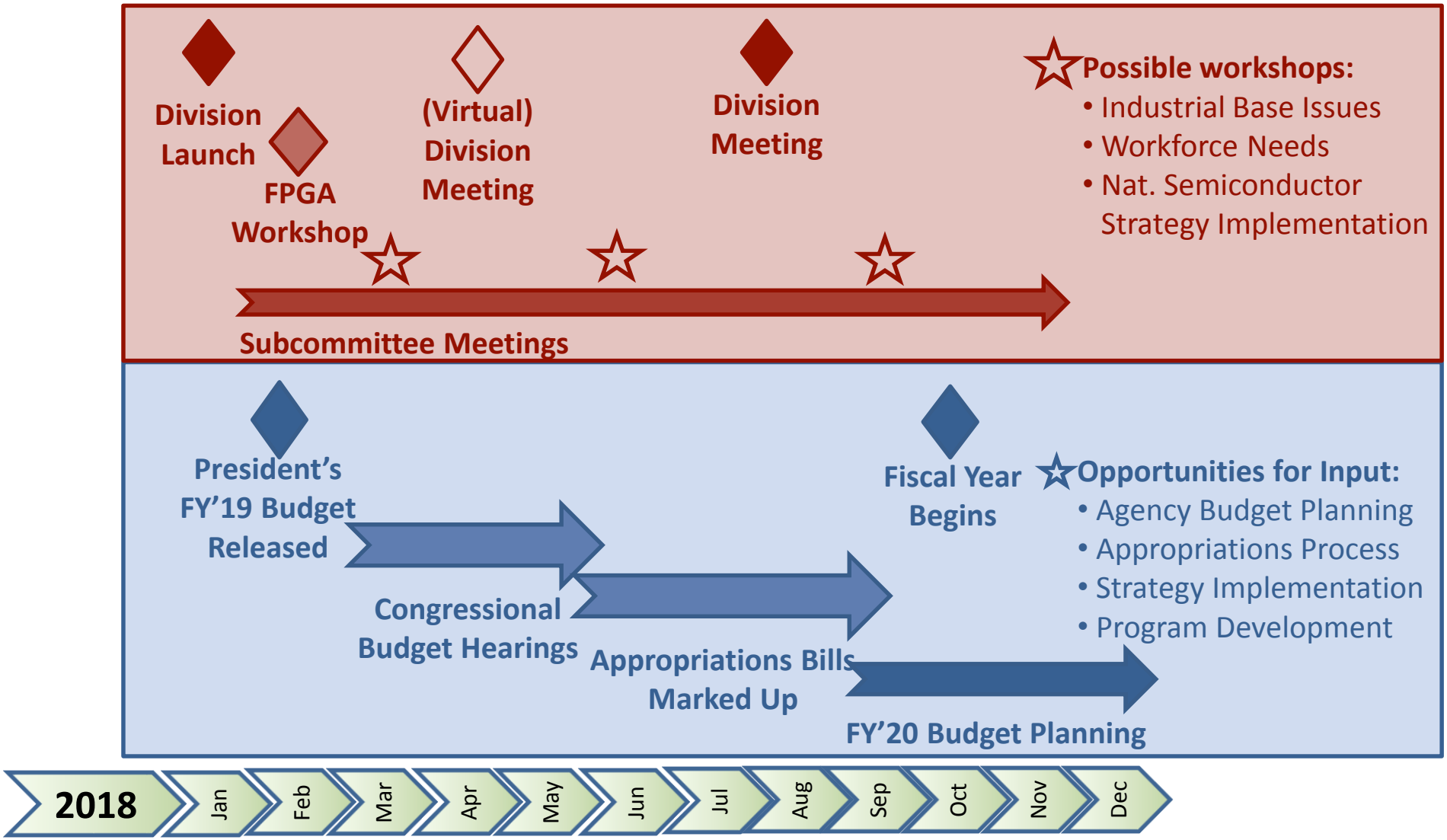
- Monthly conference calls
- Ad hoc subcommittees to address specific issues as needed
- Consensus positions, with room for dissent

We are considering all of the above, but want to hear from you.

Anita Balachandra

ACTIVITIES AND SCHEDULE

Activities & Schedule



Anita Balachandra

CALL FOR VOLUNTEERS

Kelly Hennig

WRAP UP