TRUST in Integrated Circuits Program

DARPA

MICROSYSTEMS TECHNOLOGY OFFICE

Briefing to Industry

Mr. Brian Sharkey

i_SW Corp

26 March 2007

APPROVED FOR PUBLIC RELEASE – Distribution Unlimited

Agenda

0800-0815	Introductions and Agenda	Mr. Brian Sharkey
0815-0900	Technical Objectives of the TRUST Program	Dr. Dean Collins
0900-0920	Contracts for the TRUST Program	Mr. Michael Blackstone
0920-0940	Break -- Government prepares responses to bidders first series of questions regarding Contracts, Security and Technical	
0940-0955	Teaming Website and TFIMS demonstration	Mr. Jonathan Breedlove
0955-1100	Government response to bidders questions	Dr. Dean Collins Mr. Michael Blackstone Mr. Darin Smith Ms. Jo-Anne Webber
1100-1130	Metrics for the TRUST Program	Dr. Dan Wilt
1130-1200	Plan for government provided Test Articles	Mr. Robert Parker
1200-1245	Break for Lunch	
1245-1330	Government response to any remaining technical questions	Dr. Dean Collins Mr. Michael Blackstone Mr. Darin Smith Ms. Jo-Anne Webber

BAA 07-24 POC List

- Technical Questions
  - Dean Collins
    - dean.collins@darpa.mil
    - 571-218-4650
- Contracts
  - Michael Blackstone
    - michael.blackstone@darpa.mil
    - 571-218-4804
- Security
  - Jo-Ann Webber
    - jo-ann.webber.ctr@darpa.mil
    - 571-218-4930
- FAQ / Logistics
  - Jonathan Breedlove
    - baa07-24@darpa.mil
    - 571-218-4255

Systems Integrators

POC	Organization	Email	Phone
Mark Trainoff Panchanathan Reghunathan	Raytheon	matrainoff@raytheon.com rreghunathan@raytheon.com	310-607-7346 310-647-1219
Rick Stevens Howard Schantz	Lockheed Martin	rick.c.stevens@lmco.com howard.j.schantz@lmco.com	651-456-3118 651-456-2045
Lou Paradiso Richard Plew David Mottarella	Harris Corporation	lparadis@harris.com rplew@harris.com dmottare@harris.com	321-727-5399 321-727-5399
Kenneth Heffner	Honneywell International	kenneth.h.heffner@honeywell.com	727-539-4205
Perry Koch	ARINC LLC	pkoch@arinc.com	410-266-4396

Systems Integrators

POC	Organization	Email	Phone
John Mcdonald	Rensselaer Polytechnic Institute	mcdonald@unix.cie.rpi.edu	518-276-2919
Erik Mettala	SPARTA, Inc.	Erik.Mettala@sparta.com	410-443-8059
Donna Miranda Greg Zawitoski	National Semiconductor Corp	donna.miranda@nsc.com greg.zawitoski@nsc.com	301-497-4247 301-621-0900
David Mottarella	Harris Corporation	dmottare@harris.com	321-591-8634
Jeffrey Wills	Altera Corporation	jwills@altera.com	410-750-3421

TRUST in Integrate Circuits Program

Briefing to Industry - Technical Presentation

Dr. Dean Collins

Deputy Director

Microsystems Technology Office

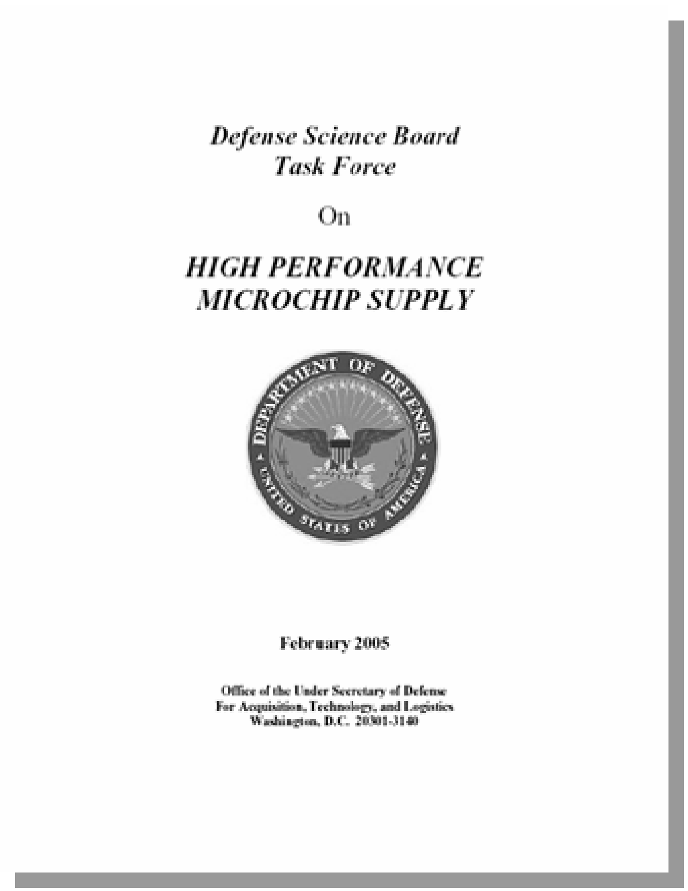
26 March 2007

Need for TRUSTed IC’s

DARPA

MICROSYSTEMS TECHNOLOGY OFFICE

High Performance Microchip Supply



Defense Science Board
Task Force

On

HIGH PERFORMANCE
MICROCHIP SUPPLY

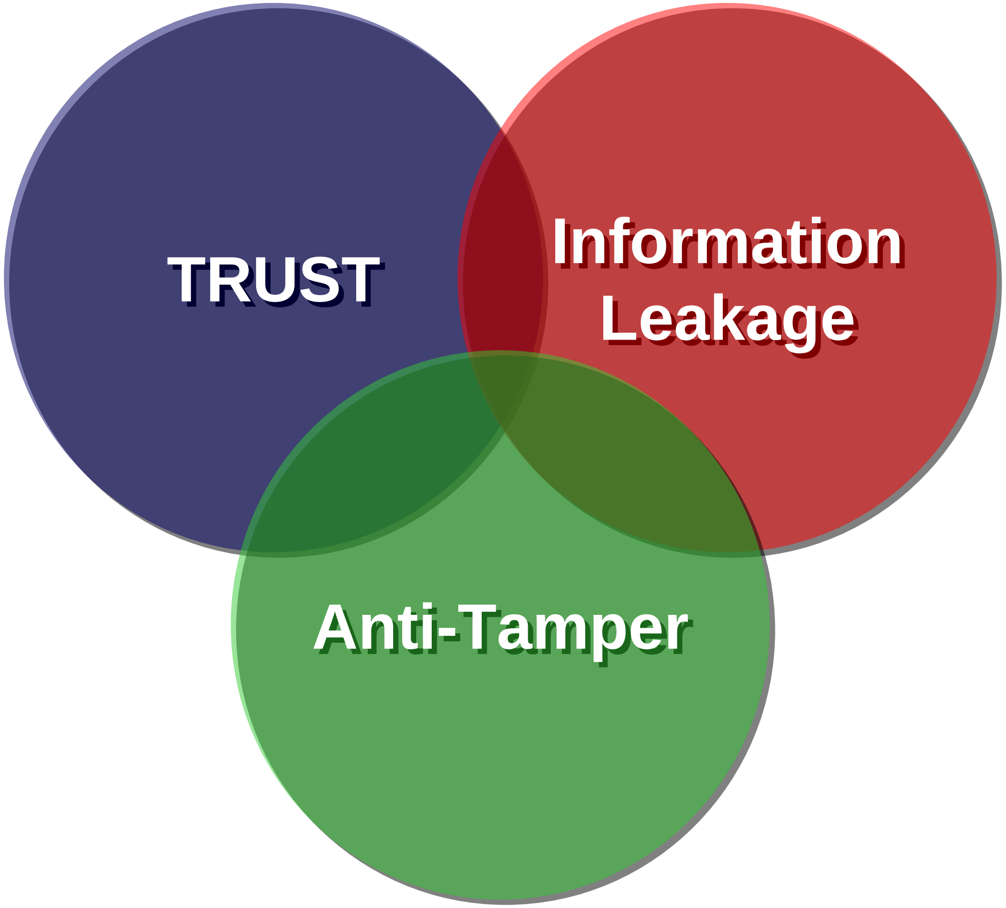
February 2005

Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140

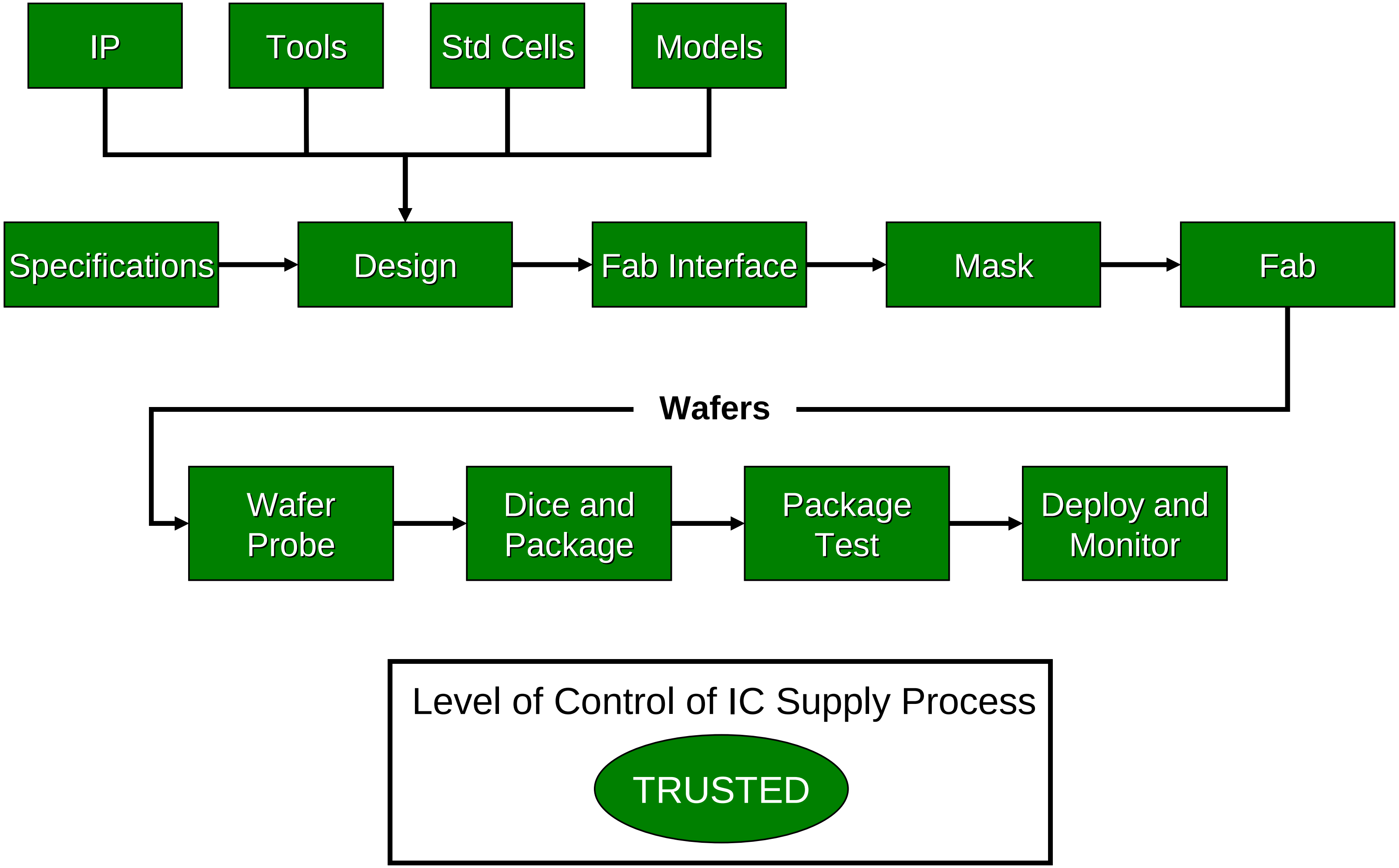
http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf

- For the DOD’s strategy of information superiority to remain viable, the Department requires:
  - Trusted, Affordable, Timely Supply of Integrated Circuits (ICs)
  - A continued stream of exponential improvements in the processing capacity of microchips and new approaches to extracting military value from information.
- Technical Aspects of Trusted Circuits:
  - Design
  - IC Fabrication
  - IC Packaging

Overlap of Interests



Old Supply Chain Structure



IP

Tools

Std Cells

Models

Specifications

Design

Fab Interface

Mask

Fab

Wafers

Wafer Probe

Dice and Package

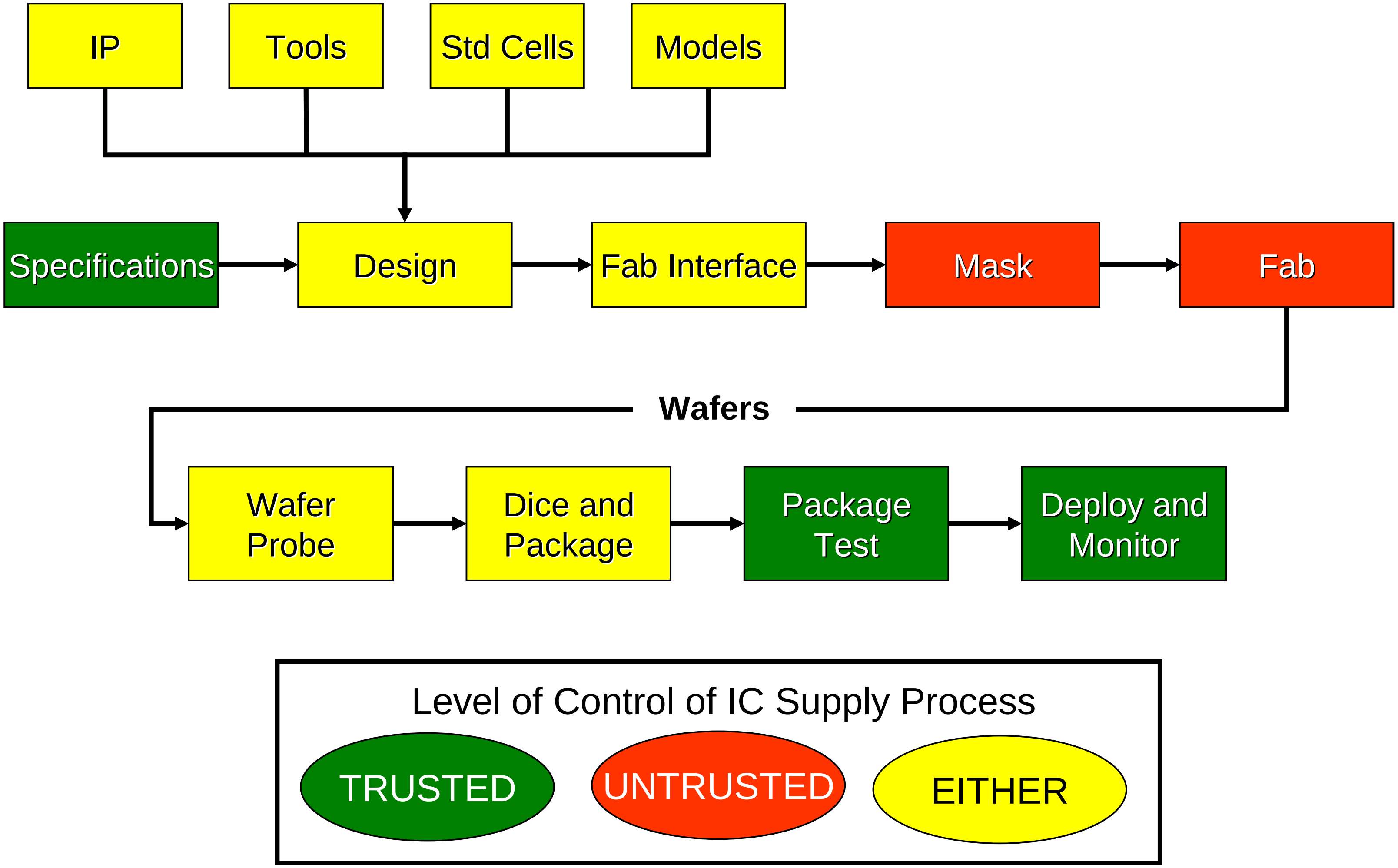
Package Test

Deploy and Monitor

Level of Control of IC Supply Process

TRUSTED

New Supply Chain Structure



IP

Tools

Std Cells

Models

Specifications

Design

Fab Interface

Mask

Fab

Wafers

Wafer Probe

Dice and Package

Package Test

Deploy and Monitor

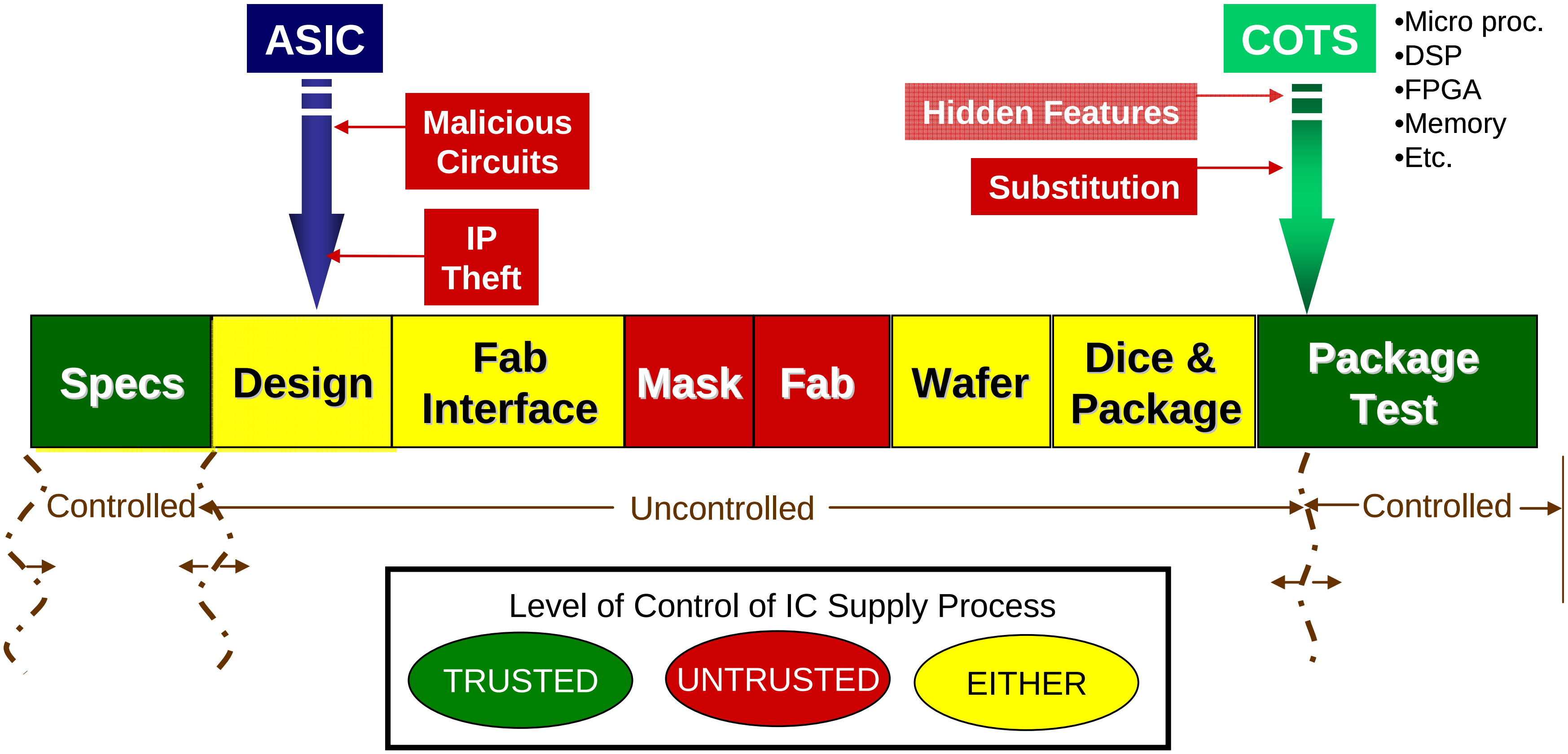
Level of Control of IC Supply Process

TRUSTED

UNTRUSTED

EITHER

Controlled and Uncontrolled Boundaries of the Chip Development Process



ASIC

Malicious Circuits

IP Theft

COTS

- Micro proc.
- DSP
- FPGA
- Memory
- Etc.

Hidden Features

Substitution

Specs | Design | Fab Interface | Mask | Fab | Wafer | Dice & Package | Package Test

Controlled ← Uncontrolled → Controlled →

Level of Control of IC Supply Process

TRUSTED

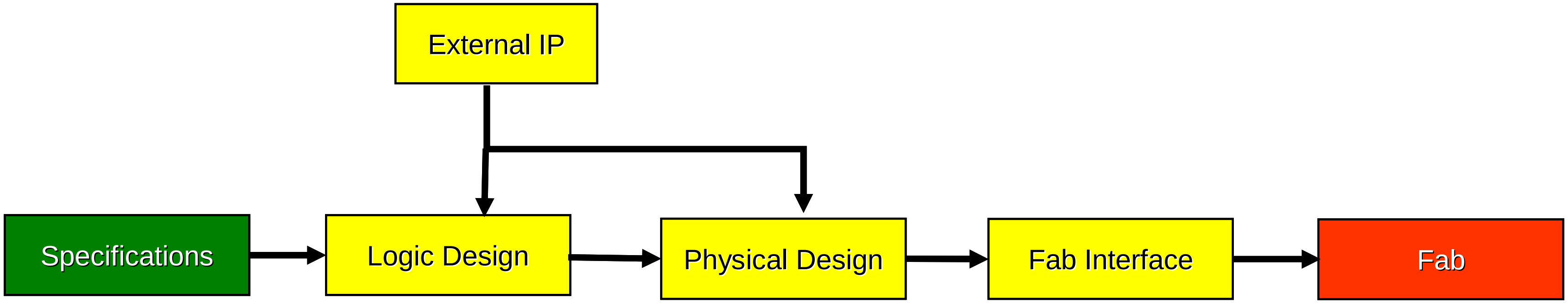
UNTRUSTED

EITHER

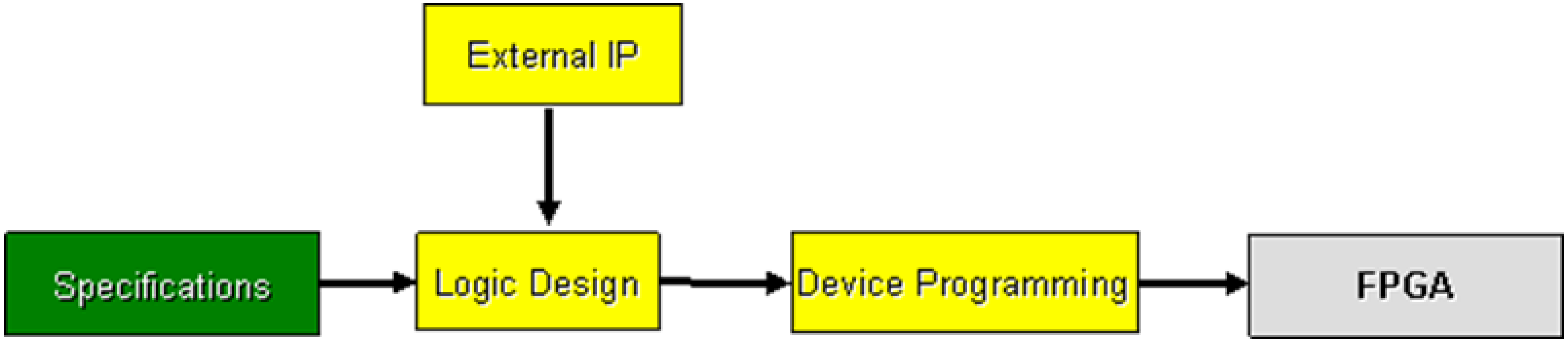
APPROVED FOR PUBLIC RELEASE – Distribution Unlimited

Type of Threats

Design Flows



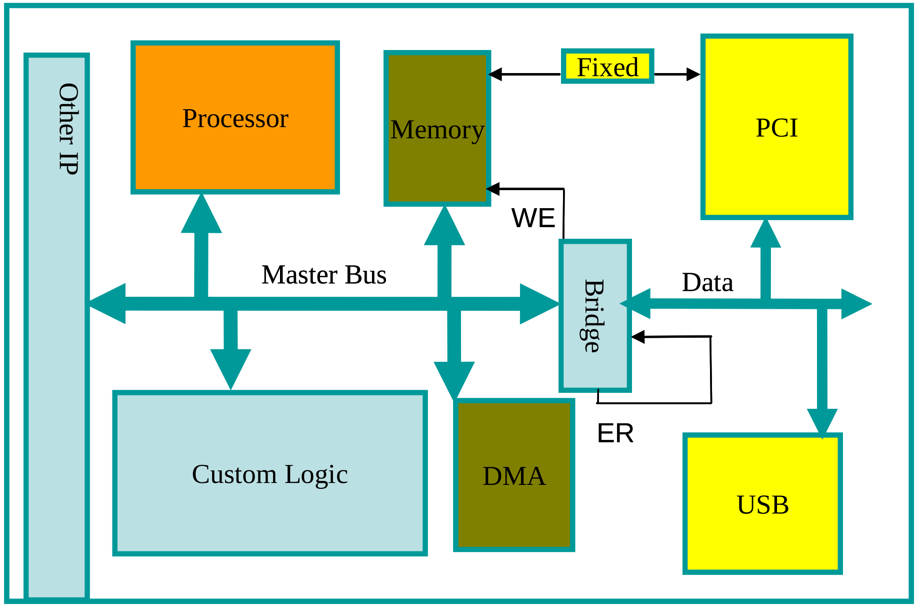
ASIC Design Flow

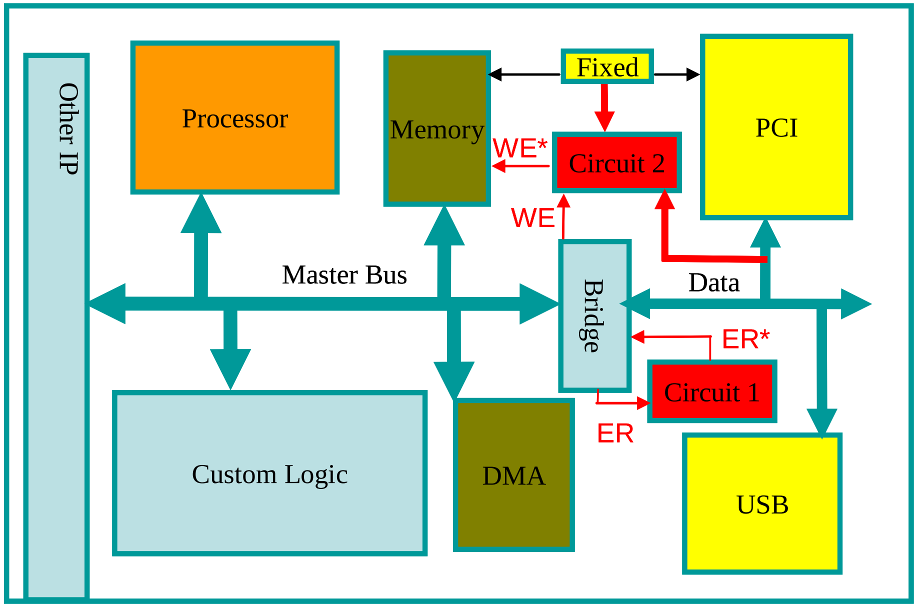


FPGA Design Flow

APPROVED FOR PUBLIC RELEASE – Distribution Unlimited

Malicious IC Insertion

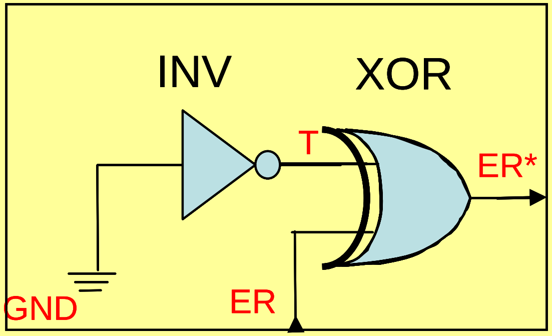




Standard IC Design

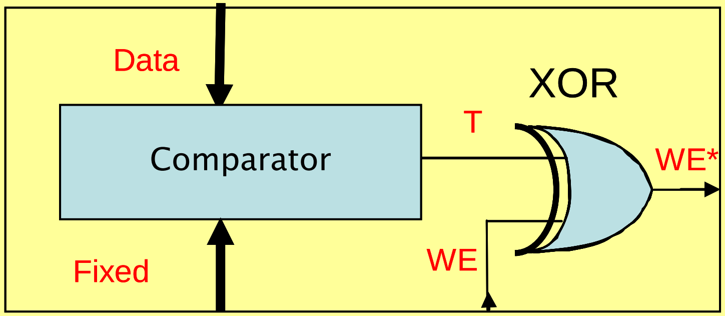
With Malicious Circuits Inserted

Example Types of Malicious Circuit Insertions



T	ER	ER*
1	0	1
1	1	0

IC Malicious Circuit 1 with Trigger Always On Condition



Data	Fixed	T	WE	WE*
232	234	0	0	0
233	234	0	1	1
234	234	1	0	1
235	234	0	0	0

IC Malicious Circuit 2 with Event Triggered Condition

Program Objectives

Area 1 – Hardware Validation

- Techniques that can quickly and accurately determine whether an IC provided is the same as one available in a gold standard design
  - Fast, accurate, high resolution destructive analysis of an IC
  - Fast, accurate, high resolution non-destructive analysis of an IC – is preferred.
  - Methods that prevent or detect the insertion of additional circuits when IC is manufactured
  - Methods for determining if IC's are identical

Area 2 – Design Validation

- Trusted Design of ASIC hardware
  - External IP
  - Logic design
  - Physical design
  - Fab interface
- Trusted design, implementation, and operation of configurable hardware, such as that provided by FPGAs
  - External IP
  - Logic design
  - Device programming

Area 3 - System Integration (SI)

- The three phases of the program are defined by technical performance goals – not time durations
  - Phase 1 – primarily proof-of-principal of individual technologies
  - Phase 2 and 3 will focus on integrating techniques into a comprehensive end-to-end system capability
  - Component providers who desire to continue to Phase 2 or 3 of the program should form teaming agreements with a system integration team prior to the end of Phase I
- System Integrator(s) will be required for Phases 2 and 3, and may also be preferred in Phase 1 in order to ensure effective coordination

Area 3 - System Integration (SI)

- System Integrator responsibilities
  - Define comprehensive TRUST solution for Area 1 and/or Area 2
  - Direction and management oversight for integrating component technology solutions into a system framework
    - System development plans,
    - Experiment plans (including milestones and go/no-go experiments),
    - Coordination of those program deliverables being produced by the technology developers
- Requirements of the SI Performer
  - Strong background in design/fabrication of complex ICs—preferably at foreign foundries
  - Strong background in the agile management of classified programs involving diverse large and small company technical performer teams
  - Success in transitioning systems and component technology products into the DoD or intelligence communities

Teaming

- Teaming is highly encouraged
- Component providers will not advance to Phase 2 or 3 without being part of a system integration team
- Non-formalized working relationships are not of interest nor are separate technical efforts that rely on each other in order to provide a solution

Teaming

- FAQ: "Given the inherent increase in risk associated with a team approach that is not structured as with a formal prime/sub arrangement, formal teaming agreement(s) must be provided as part of the proposal submission(s) in such instances. The lack of such agreements would be considered as an unacceptable level of risk during evaluations of Tech Area 1 and 2"
  - The lack of such teaming agreements may be considered an unacceptable risk
  - It is recognized that there may not be sufficient time for formal teaming agreements to be executed prior to submission of proposals lacking a prime/sub relationship
  - Proposers should provide evidence that formal teaming agreements will be in place prior to contract award

Security Considerations

- Continued research on some technologies developed under this program may require security protection in order to continue, especially when integrated within a broader system framework
- DARPA has determined that research resulting from this program will present a high likelihood of disclosing performance characteristics of military systems or manufacturing technologies that are unique and critical to defense; therefore, any resulting award will include a requirement for DARPA permission before publishing any information or results on the program.

Technical Goals and Schedule

Government Support Teams

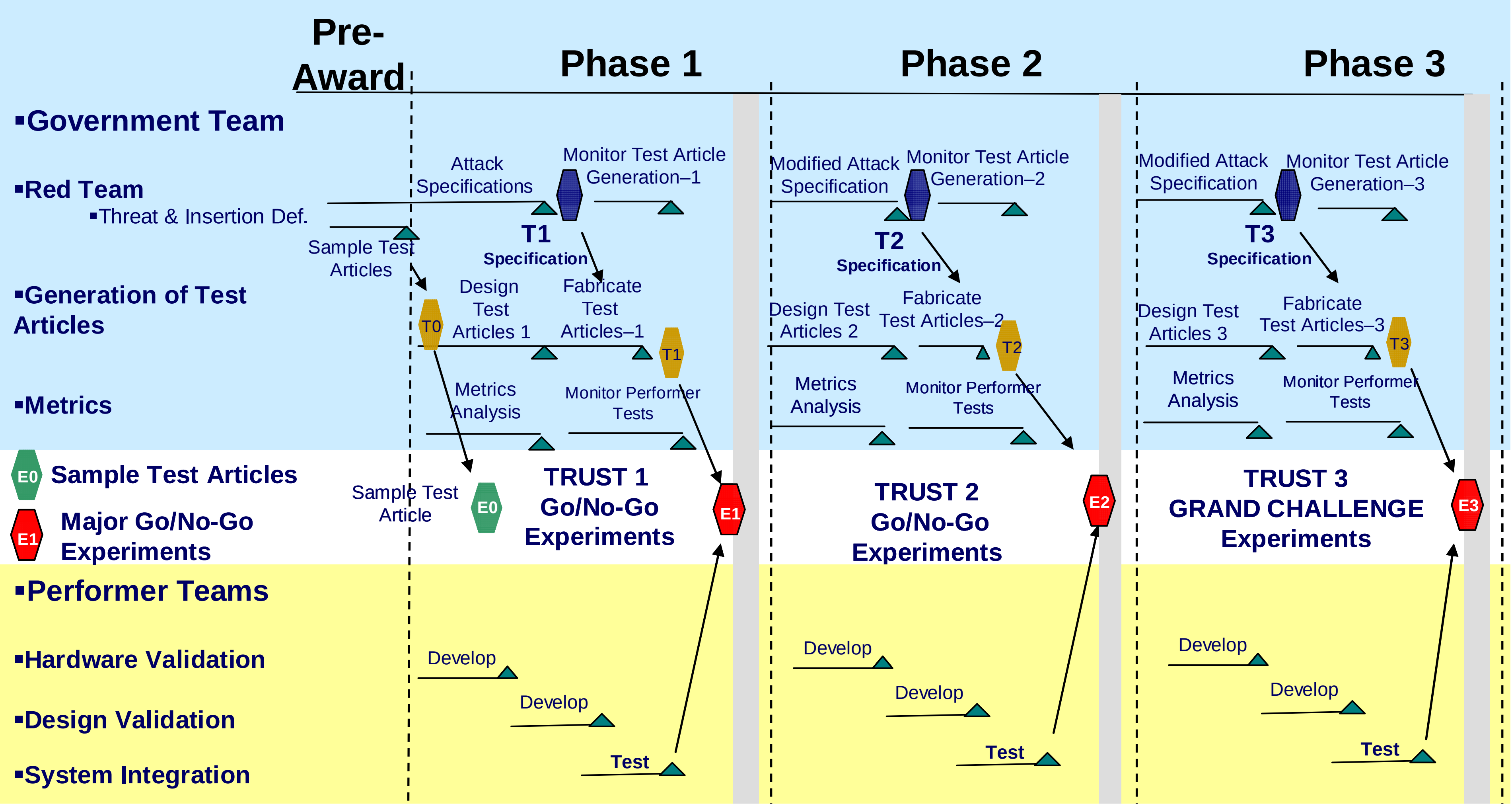
- Red Team
  - Led by MIT- LL
  - Identify different classes of malicious circuits
  - Establish techniques for malicious circuit insertion within test articles
- Test Article Generation
  - Led by USC- ISI
  - Will use MOSIS to access commercial foundries to generate HW test articles
  - Will use standard design tool applications for design SW test articles.
- Metrics Team
  - John Hopkins University – Applied Physics Laboratory
    - Methodology for establishing metrics at the transistor and IC level
    - Work with performing contractors to vet and formalize metrics established for Go/No-go experiments

TRUST Program Goals (transistor level metrics)

Process	Area 1—Hardware Validation Case 1 Trusted Design and Untrusted FAB			Area 2—Design Validation Case 2 Untrusted Design ASIC			Area 2—Design Validation Case 3 Untrusted Design FPGA		
	Phase 1	Phase 2	Phase 3	Phase 1	Phase 2	Phase 3	Phase 1	Phase 2	Phase 3
P_D	90.0%	99.0%	99.9%	80.0%	90.0%	99.0%	90.0%	99.0%	99.9%
P_{FA}	10^{-3}	10^{-5}	10^{-7}	10^{-3}	10^{-4}	10^{-6}	10^{-3}	10^{-5}	10^{-6}
# of Transistors Evaluated	10^5	10^6	10^8	10^5	10^6	10^8	10^5	10^6	10^7
Time to Evaluate*	480 H	240 H	120 H	480 H	240 H	120 H	480 H	240 H	120 H

**Combined man hours plus wall clock time.*

TRUST Program Schedule



Pre-Award

Phase 1

Phase 2

Phase 3

- Government Team
- Red Team
  - Threat & Insertion Def.
- Generation of Test Articles
- Metrics

E0 Sample Test Articles

E1 Major Go/No-Go Experiments

- Performer Teams
- Hardware Validation
- Design Validation
- System Integration

Attack Specifications

Monitor Test Article Generation–1

T1 Specification

Sample Test Articles

Design Test Articles 1

Fabricate Test Articles–1

T0

T1

Metrics Analysis

Monitor Performer Tests

Sample Test Article

E0

TRUST 1 Go/No-Go Experiments

E1

Develop

Develop

Test

Modified Attack Specification

Monitor Test Article Generation–2

T2 Specification

Design Test Articles 2

Fabricate Test Articles–2

T2

Metrics Analysis

Monitor Performer Tests

TRUST 2 Go/No-Go Experiments

E2

Develop

Develop

Test

Modified Attack Specification

Monitor Test Article Generation–3

T3 Specification

Design Test Articles 3

Fabricate Test Articles–3

T3

Metrics Analysis

Monitor Performer Tests

TRUST 3 GRAND CHALLENGE Experiments

E3

Develop

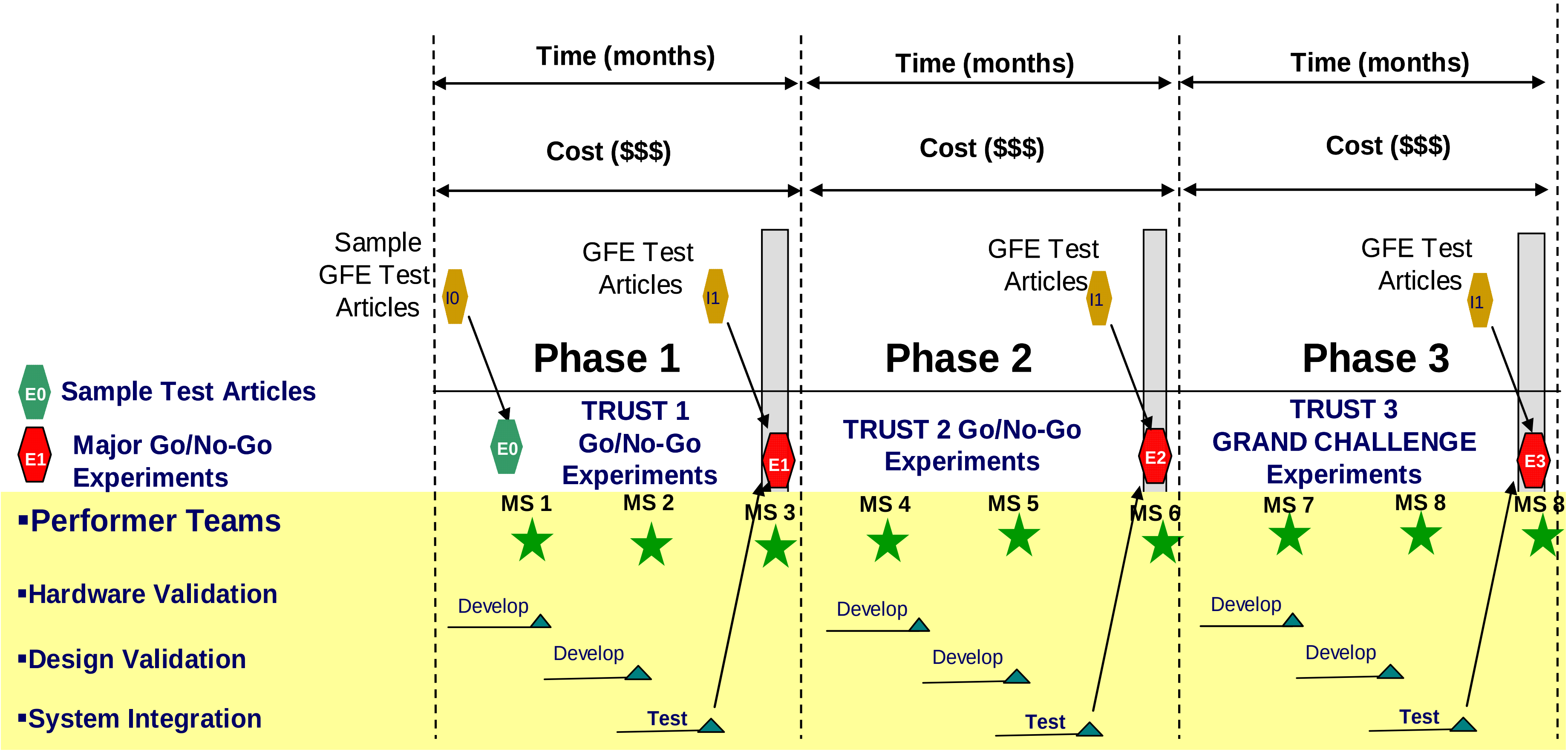
Develop

Test

APPROVED FOR PUBLIC RELEASE – Distribution Unlimited

Proposal Requirements

Contractor Proposed Milestone Schedule



E0 Sample Test Articles

E1 Major Go/No-Go Experiments

Sample GFE Test Articles

I0

GFE Test Articles

I1

Time (months)

Cost ($$$)

Phase 1

E0

TRUST 1 Go/No-Go Experiments

E1

Time (months)

Cost ($$$)

GFE Test Articles

I1

Phase 2

TRUST 2 Go/No-Go Experiments

E2

Time (months)

Cost ($$$)

GFE Test Articles

I1

Phase 3

TRUST 3 GRAND CHALLENGE Experiments

E3

- Performer Teams
- Hardware Validation
- Design Validation
- System Integration

MS 1 ★

MS 2 ★

MS 3 ★

MS 4 ★

MS 5 ★

MS 6 ★

MS 7 ★

MS 8 ★

Develop

Develop

Test

Develop

Develop

Test

Develop

Develop

Test

Time duration of phases is to be determined by the proposer.

Key Assumptions

Key Assumption	Explanation
To what element(s)/process step(s) of the process flow does each technique pertain? See Figure 3.	
Is the technique applicable to ASICs and/or COTS (FPGAs)?	
What are the inputs required and output set of information created?	
With regard to the controlled and uncontrolled boundaries shown in Figure 3, what parts of the process are better controlled because of your technique?	
What is the insertion point of the technique?	
What are the measurement points to determine the effectiveness of the technique?	
Is a gold standard assumed? By this we mean that there is a preserved reference item of a known trusted design or manufactured part that can be used to assess the trust of the item in question.	

Contractor Proposed Experimental Goals

Process	Area 1—Hardware Validation Case 1 Trusted Design and Untrusted FAB			Area 2—Design Validation Case 2 Untrusted Design ASIC			Area 2—Design Validation Case 3 Untrusted Design FPGA		
	Phase 1	Phase 2	Phase 3	Phase 1	Phase 2	Phase 3	Phase 1	Phase 2	Phase 3
P_D									
P_{FA}									
# of Transistors Evaluated	10^5	10^6	10^8	10^5	10^6	10^8	10^5	10^6	10^7
Time to Evaluate*									

** Combined man hours plus wall clock time*

Task Breakdown

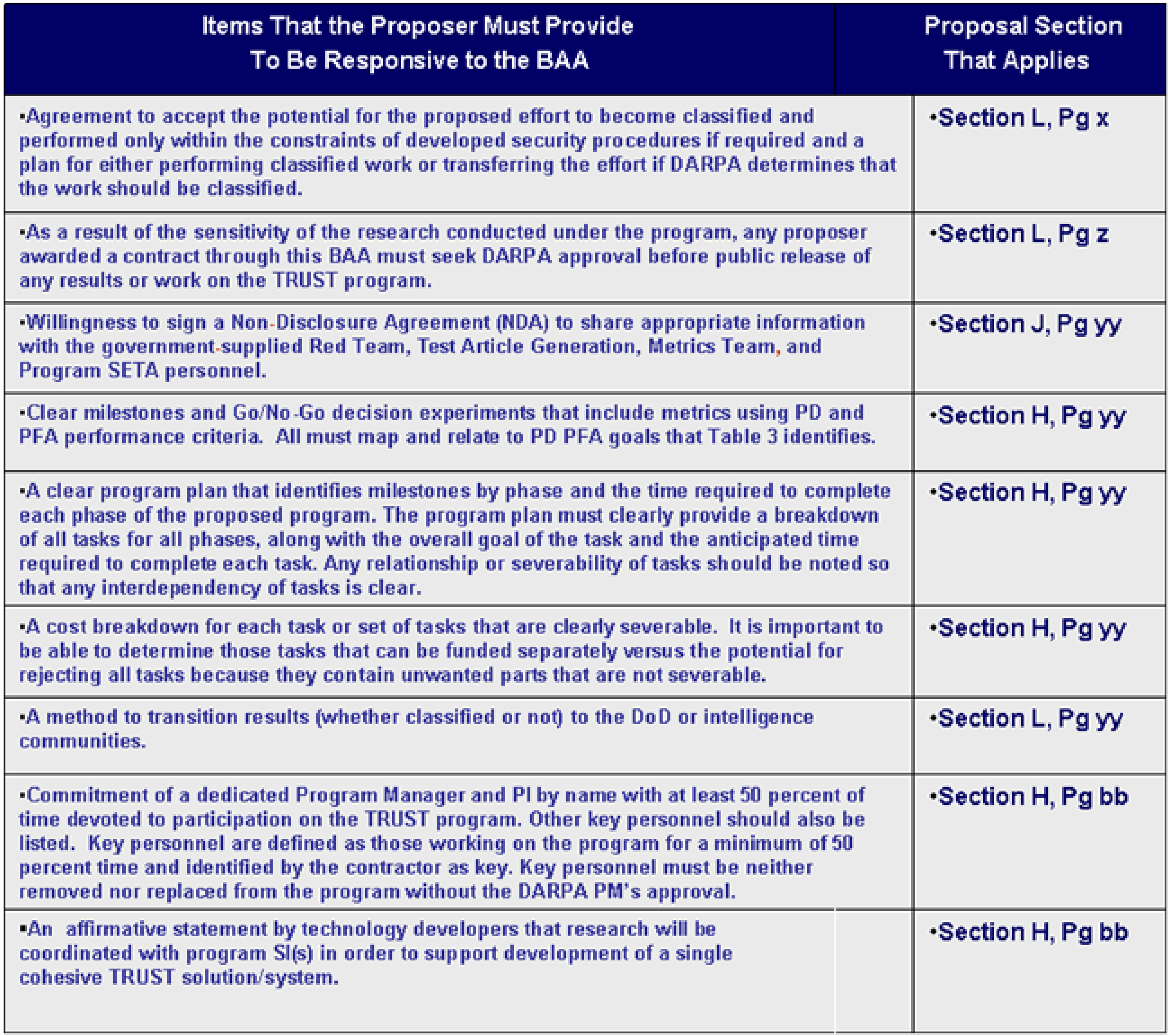
- The technical effort must be defined with sufficient granularity to enable DARPA to select part of the work if desired
- Identify which tasks/subtasks are severable and which tasks/subtasks have interdependency
- Each severable task/subtask must have individual metrics-based goals for each of the defined phases
- Costs must be defined at the Task/Sub-task level and for each program phase

DARPA may reject an entire proposal if there is insufficient granularity of costs and goals for the individual tasks proposed

Program Plan Matrix

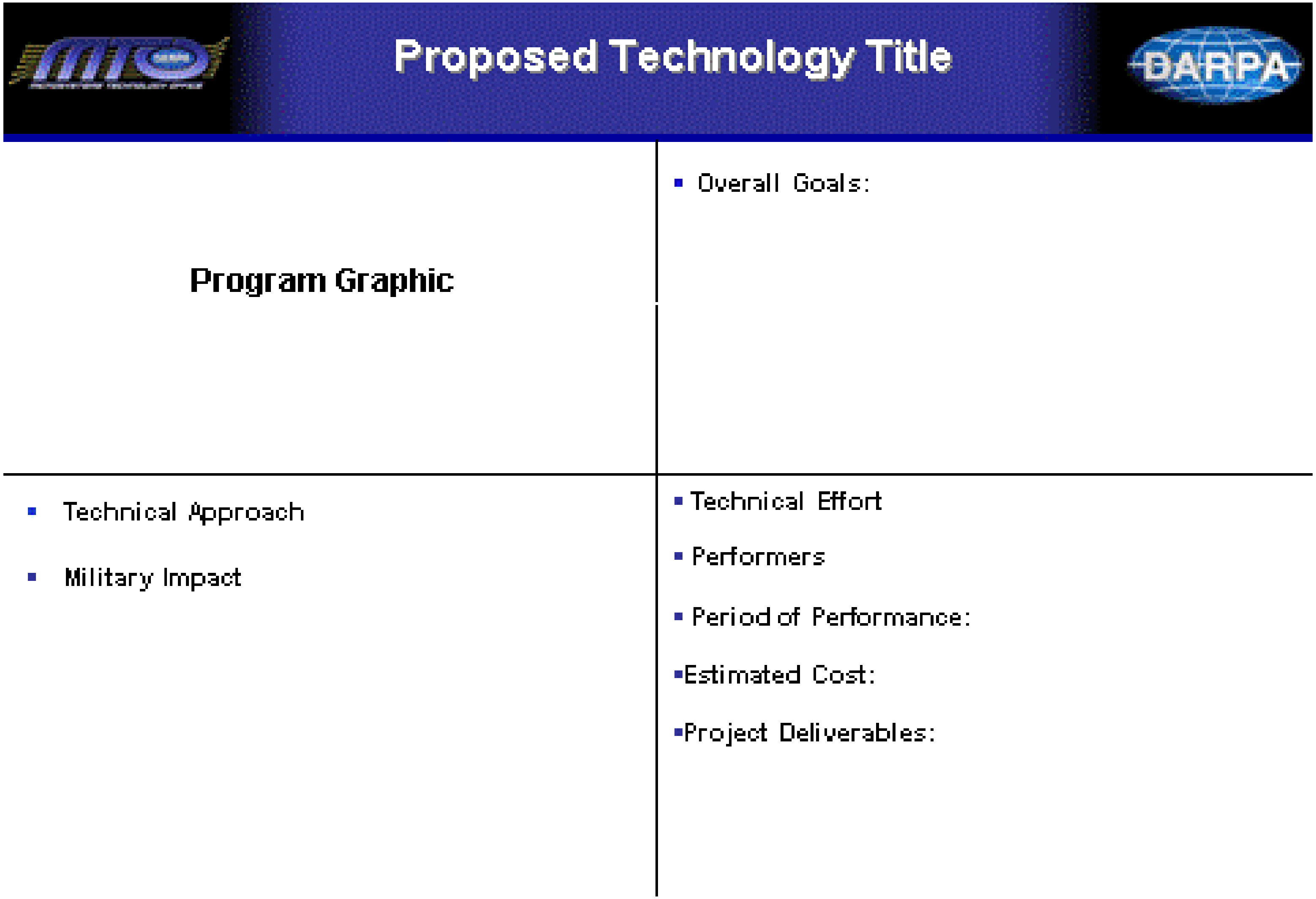
Phase	Task	Description of Work	Total Cost	Cost Breakdown	Go/No Go Criteria	Expected Go/No-Go Definitions	Deliverables	Task Interdependencies	Key Personnel
Phase I	A			Labor $, M&S $, Sub $	Pd, Pfa, Time, Cost, Etc.				
	B				Pd,Pfa, T,C				
	C				Pd, Pfa, T,C				
Phase Total									
Phase II	A				Pd, Pfa, T, C				
	B				Pd, Pfa, T, C				
	C				Pd, Pfa, T, C				
Phase Total									
Phase II	A				Pd, Pfa, T, C				
	B				Pd, Pfa, T, C				
	C				Pd, Pfa, T,C				
Phase Total									
Total									

Items Required
to be Responsive to the BAA



Items That the Proposer Must Provide To Be Responsive to the BAA	Proposal Section That Applies
•Agreement to accept the potential for the proposed effort to become classified and performed only within the constraints of developed security procedures if required and a plan for either performing classified work or transferring the effort if DARPA determines that the work should be classified.	•Section L, Pg x
•As a result of the sensitivity of the research conducted under the program, any proposer awarded a contract through this BAA must seek DARPA approval before public release of any results or work on the TRUST program.	•Section L, Pg z
•Willingness to sign a Non-Disclosure Agreement (NDA) to share appropriate information with the government-supplied Red Team, Test Article Generation, Metrics Team, and Program SETA personnel.	•Section J, Pg yy
•Clear milestones and Go/No-Go decision experiments that include metrics using PD and PFA performance criteria. All must map and relate to PD PFA goals that Table 3 identifies.	•Section H, Pg yy
•A clear program plan that identifies milestones by phase and the time required to complete each phase of the proposed program. The program plan must clearly provide a breakdown of all tasks for all phases, along with the overall goal of the task and the anticipated time required to complete each task. Any relationship or severability of tasks should be noted so that any interdependency of tasks is clear.	•Section H, Pg yy
•A cost breakdown for each task or set of tasks that are clearly severable. It is important to be able to determine those tasks that can be funded separately versus the potential for rejecting all tasks because they contain unwanted parts that are not severable.	•Section H, Pg yy
•A method to transition results (whether classified or not) to the DoD or intelligence communities.	•Section L, Pg yy
•Commitment of a dedicated Program Manager and PI by name with at least 50 percent of time devoted to participation on the TRUST program. Other key personnel should also be listed. Key personnel are defined as those working on the program for a minimum of 50 percent time and identified by the contractor as key. Key personnel must be neither removed nor replaced from the program without the DARPA PM's approval.	•Section H, Pg bb
•An affirmative statement by technology developers that research will be coordinated with program SI(s) in order to support development of a single cohesive TRUST solution/system.	•Section H, Pg bb

Template for Quad Chart



Proposed Technology Title

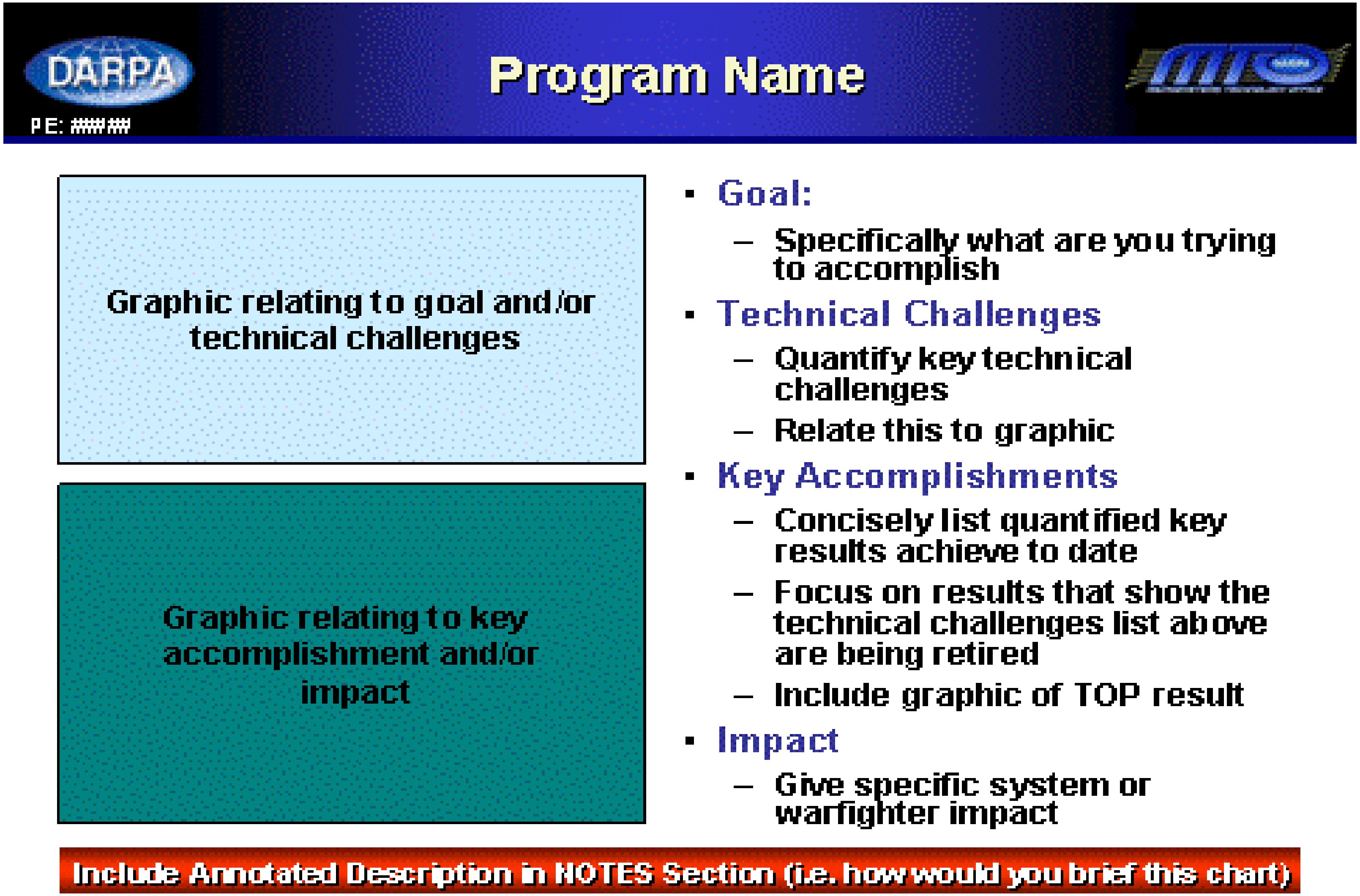
Program Graphic

- Overall Goals:

- Technical Approach
- Military Impact

- Technical Effort
- Performers
- Period of Performance:
- Estimated Cost:
- Project Deliverables:

Sample Slide Format
Explaining Technical Proposal



Program Name

PE: #####

Graphic relating to goal and/or technical challenges

Graphic relating to key accomplishment and/or impact

- Goal:
  - Specifically what are you trying to accomplish
- Technical Challenges
  - Quantify key technical challenges
  - Relate this to graphic
- Key Accomplishments
  - Concisely list quantified key results achieve to date
  - Focus on results that show the technical challenges list above are being retired
  - Include graphic of TOP result
- Impact
  - Give specific system or warfighter impact

Include Annotated Description in NOTES Section (i.e. how would you brief this chart)

Question Process

- Please write your questions down on 3” x 5” cards
- Place the question category at the top
- Place your questions in the box out on the registration table
- We will attempt to answer as many questions as time will allow
- Answers to all questions will be posted on the BAA 07-24 FAQ page
- www.darpa.mil/mto/solicitations/baa07-24/index.html

APPROVED FOR PUBLIC RELEASE – Distribution Unlimited