Supply Chain Risk Management (SCRM), Cybersecurity (CS) & "White-Listing"

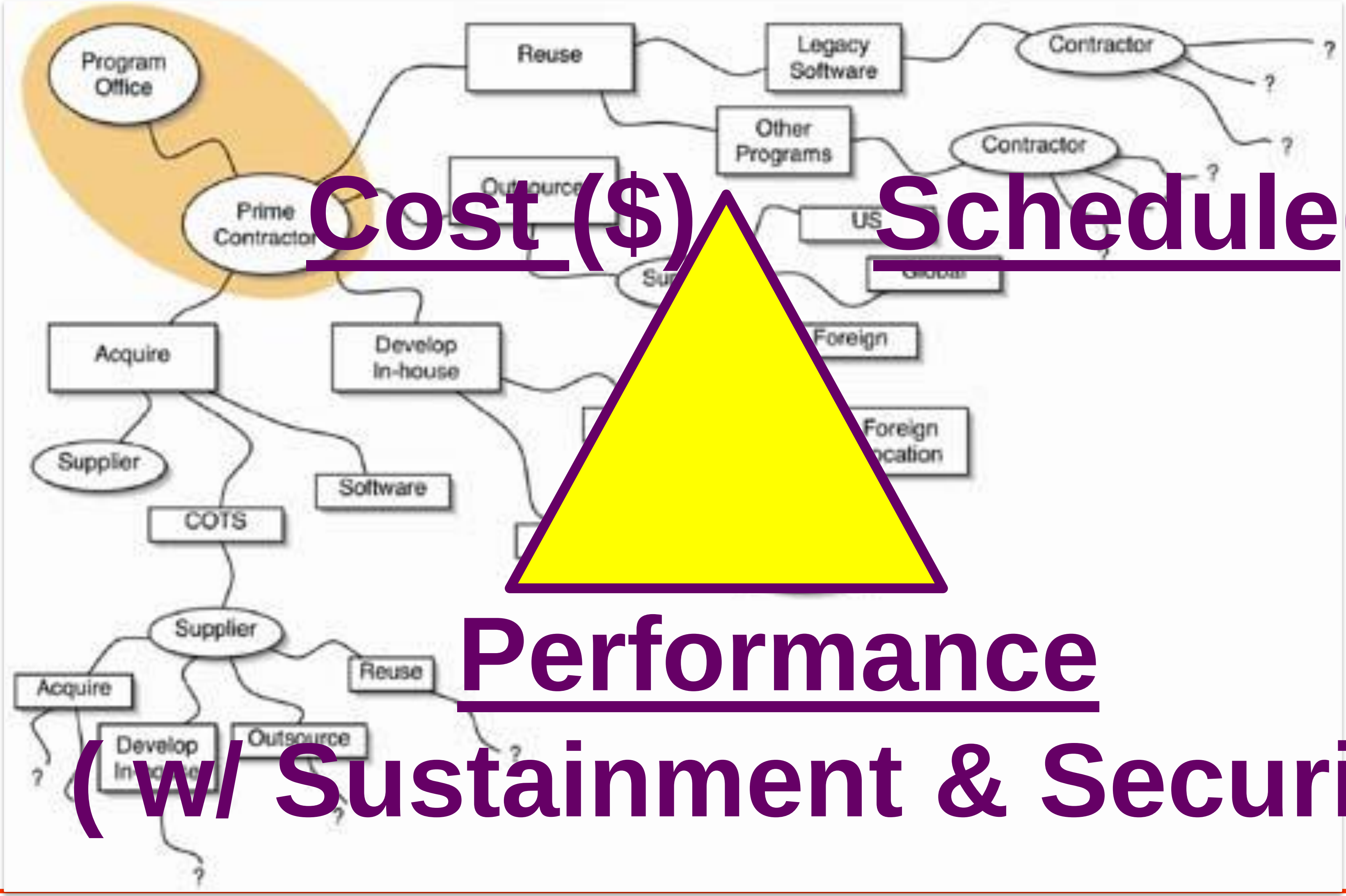
Don Davidson

Deputy Director, CS Implementation and CS/Acquisition Integration Division
Office of the Deputy DoD-CIO for Cybersecurity

26 October 2016

NDIA Systems Engineering Conference

Globalization is good, but it brings challenges



Cost ($) **Schedule(t)**

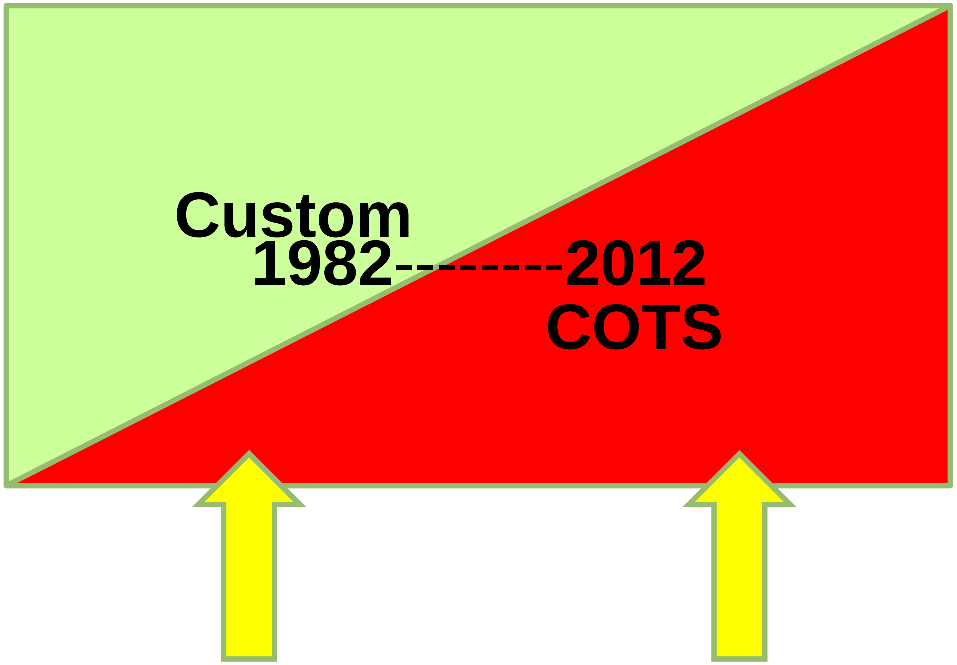
Performance

(w/ Sustainment & Security)

Increasing Dependency on COTS Creates Opportunities and Challenges

Opportunities

- ❑ Increased Use of Innovative Technology
- ❑ Faster Time to Deployment
- ❑ Continuous Cyber And Functionality Updates On Supported Technologies
- ❑ Increased use of Global ICT Standards



Challenges

- ❑ Decreased visibility into development practices
- ❑ Decreased Control of Lower Tier Suppliers
- ❑ Decreased Level Of Detail In Product Requirements And Testing

"This is a trend the department has frankly been willing to recognize more in policy than in practice…I'd hazard a guess that 25 years ago, 70 percent of the goods and services the department procured were developed and produced exclusively for the military. Today, that ratio has reversed. Seventy percent of our goods and services are now either produced for commercial consumption or with commercial applications in mind. And it's backed by a largely commercial-based supply chain."

– Mr Brett Lambert, former DASD for Manufacturing and Industrial Base Policy

Supply Chain: PERSPECTIVES

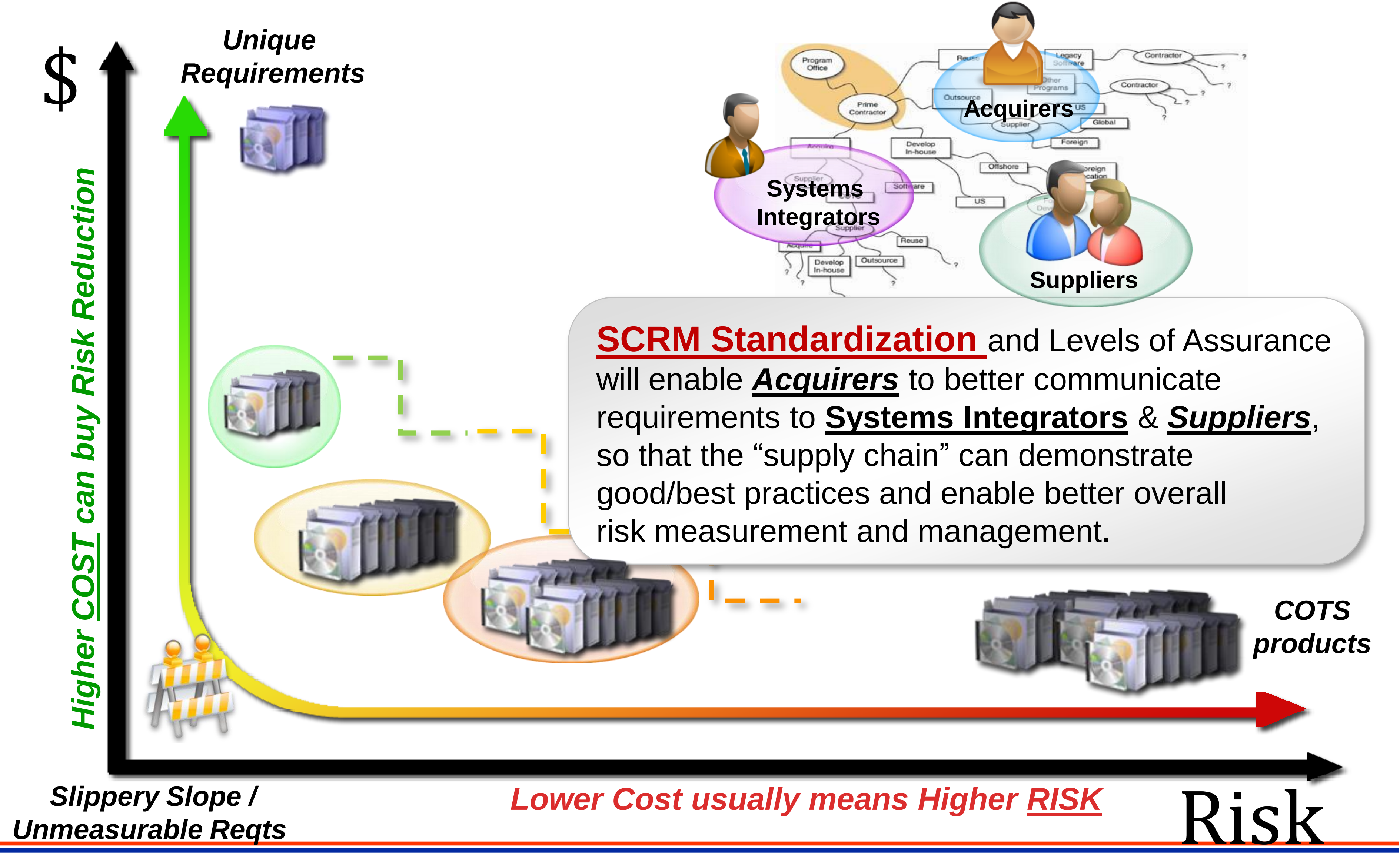
Supply Chain SECURITY & RESILIENCY are important but we are mostly focused on

Product INTEGRITY

How do we improve our trust & confidence in HW, SW & Services we source from a global supply chain?

… and more recently more emphasis on ***data protection*** *with supply chain partners.*

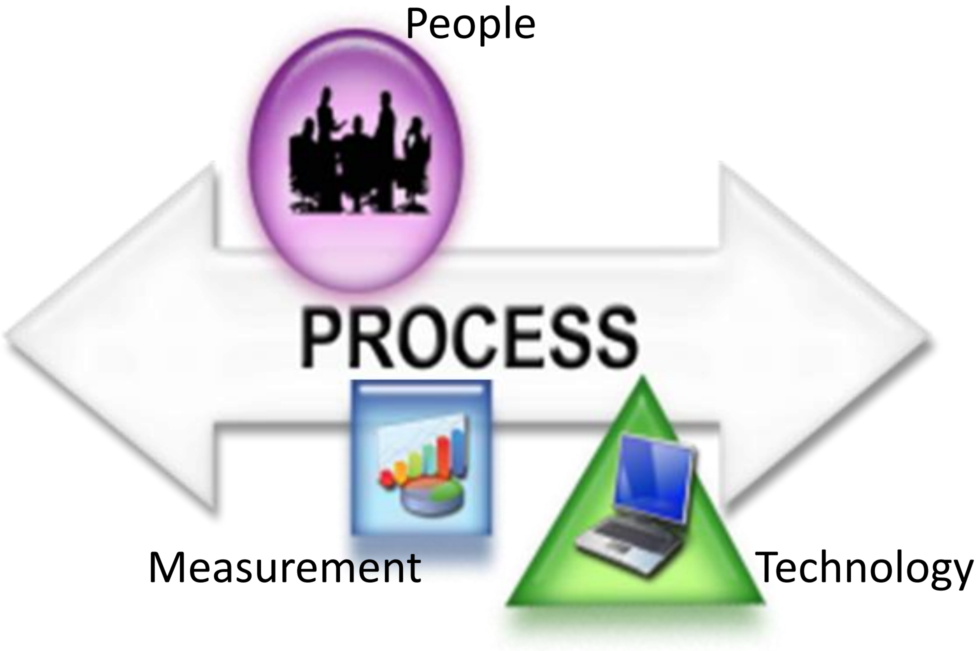
Product Assurance *TRADESPACE*



SCRM Standardization and Levels of Assurance will enable ***Acquirers*** to better communicate requirements to **Systems Integrators** & ***Suppliers***, so that the "supply chain" can demonstrate good/best practices and enable better overall risk measurement and management.

There is a need to develop the

Science of Cybersecurity



We need to better understand how to measure cybersecurity / cyber risk?

ISO/IEC 27002

Confidentiality=
Ensuring that information is accessible only to those authorized to have access.

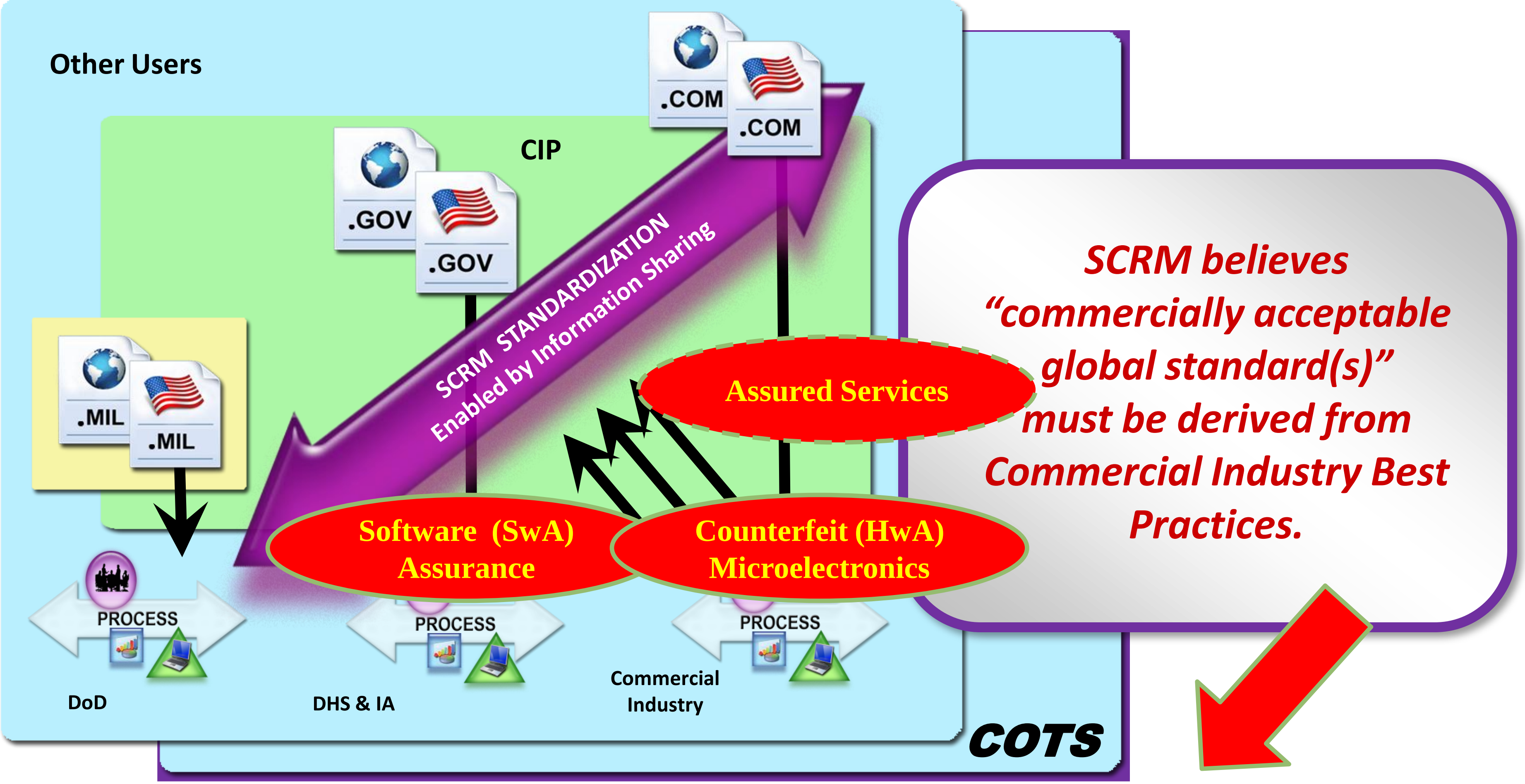
Integrity=
Safeguarding the accuracy and completeness of information and processing methods.

Availability=
Ensuring that authorized users have access to information and associated assets when required.

(Leader Awareness….. ICT as new Insider Threat)

SCRM has a Landscape of Activities & must address Counterfeits & Software (& Assured Services)

US has vital interest in the global supply chain.



SCRM believes "commercially acceptable global standard(s)" must be derived from Commercial Industry Best Practices.

SCRM Standardization Requires Public-Private Collaborative Effort

SCRM informs Us
(and our decision making processes)

Given: We rely more & more on COTS / modular components (microelectronic & software), that are supplied through a globally sourced supply chain.

What information is needed for our

“Make-or-Buy” decision,

&

how do we make our

“Fit-for-Use” determination?

Ensure DoD Missions (and critically enabling systems) are DEPENDABLE in the face of cyber warfare by a capable cyber adversary.

- Our DoD Trusted Defense Systems Strategy, is codified in DoD Instruction 5200.44, "Protection of Mission- Critical Functions to Achieve Trusted Systems and Networks (TSN)."

- ***Microelectronics Security & Trusted Foundries***

  &

- ***Software Assurance***

  are sub-elements (foundational building blocks) of our strategy.

2013 Executive Order 13636 & the Cybersecurity Framework for Critical Infrastructure Protect

Section 8(e) Report / EO 13636

- The Final Report, "*Improving Cybersecurity and Resilience through Acquisition*," was publicly released January 23, 2014: (http://gsa.gov/portal/content/176547)
- Recommends six acquisition reforms:
  I. Institute **Baseline Cybersecurity Requirements** as a Condition of Contract Award for Appropriate Acquisitions

  II. Address **Cybersecurity in Relevant Training**

  III. Develop **Common Cybersecurity Definitions** for Federal Acquisitions

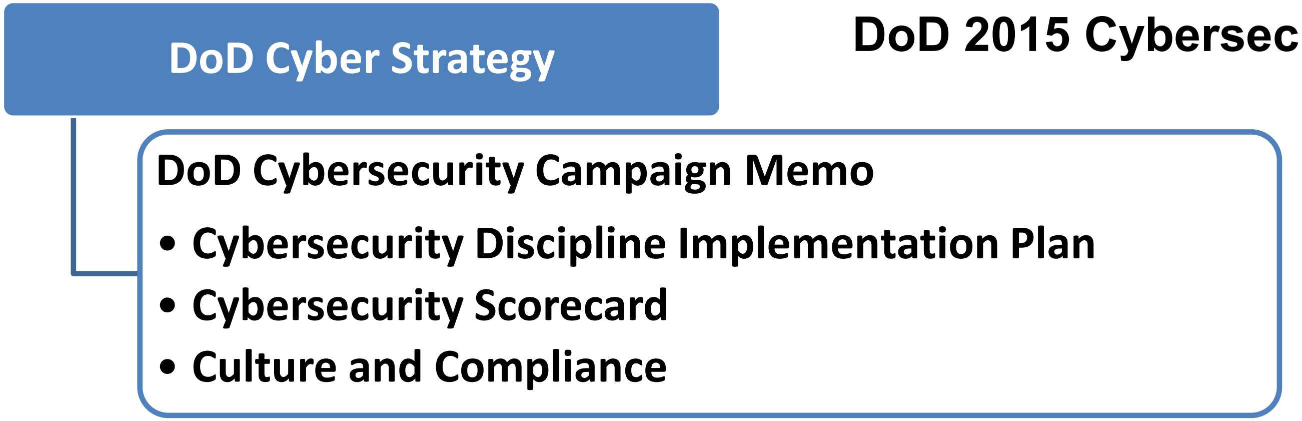
  IV. Institute a **Federal Acquisition Cyber Risk Management Strategy**

  V. Include a Requirement to **Purchase from Original Equipment Manufacturers**, Their Authorized Resellers, or Other "Trusted" Sources, Whenever Available, in Appropriate Acquisitions

  VI. Increase **Government Accountability for Cyber Risk Management**

Ultimate goal of the recommendations is to strengthen the federal government's cybersecurity by improving management of the people, processes, and technology affected by the Federal Acquisition System

DoD 2015 Cybersecurity “push”



DoD Cyber Strategy

DoD Cybersecurity Campaign Memo

- Cybersecurity Discipline Implementation Plan
- Cybersecurity Scorecard
- Culture and Compliance

DoD Cyber Strategy and Implementation Plan issued by the Principal Cyber Advisor--eight different lines of effort across the Department (April 2015)

➢ **Cybersecurity Campaign Memo** Tri-signed by DoD CIO, USD (AT&L) and Commander, CYBERCOM on June 12, 2015-announces the initiation of a multi-faceted campaign (reinforced by Operation CYBER SHIELD)

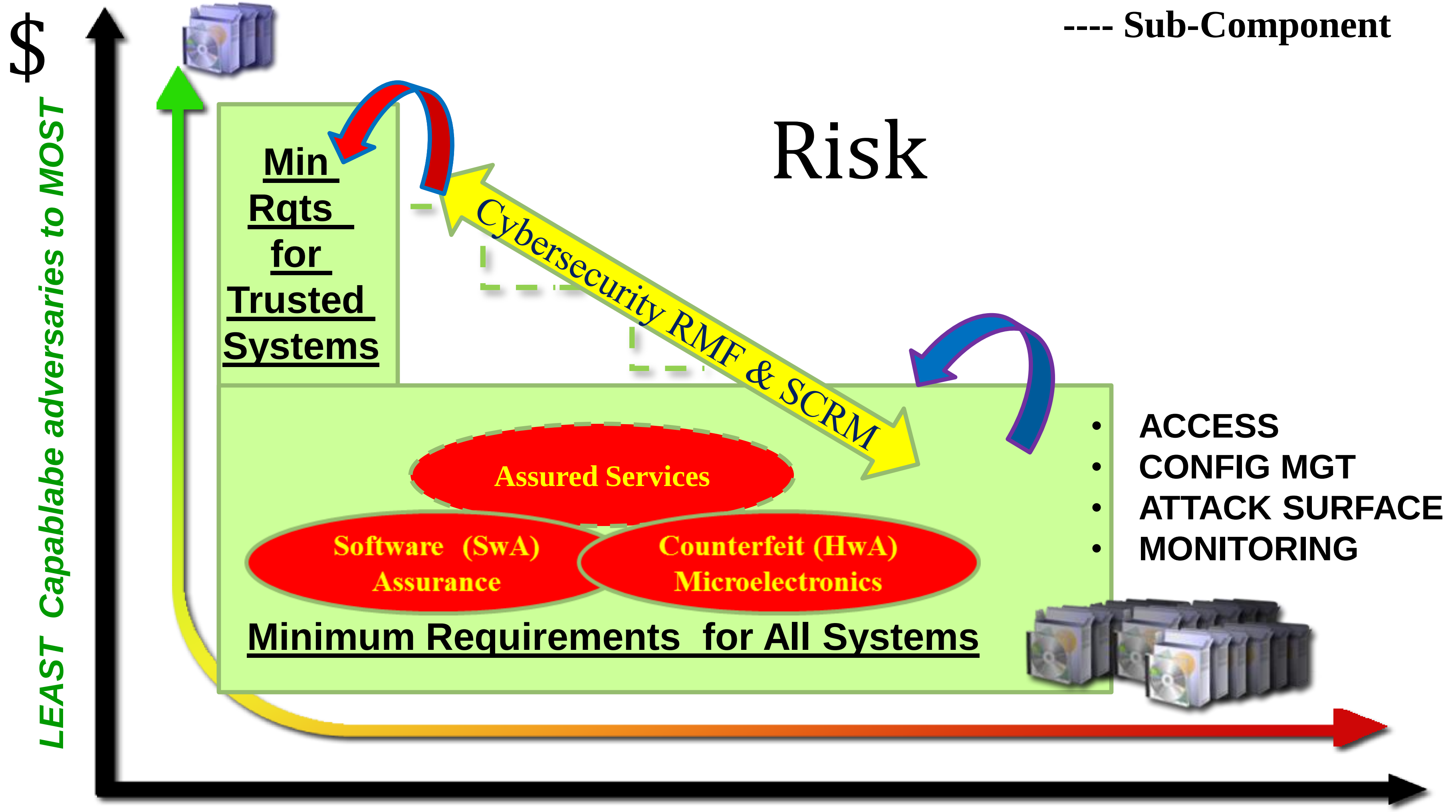
- **Cybersecurity Discipline Implementation Plan** just Oct/Nov’15 signed by DepSecDef and VCJCS--gives detailed guidance on the Cybersecurity Campaign
- **Cybersecurity Scorecard** the visual presentation of ten basic cybersecurity metrics of the Department--delivered monthly since June 2015 ***(Cybersecurity Scorecard Evolution)*** is an in-progress adaptation of the current scorecard efforts to include more comprehensive data collection and metrics on cyber basics and programs of record in development
- **DoD Cybersecurity Culture and Compliance** signed out September 30, 2015 by SECDEF and CJCS--a multi-faceted initiative to raise the level of human awareness, performance and accountability in cybersecurity.

Cybersecurity Discipline Implementation Plan signed by DepSecDef and VCJCS—gives detailed guidance on the Cybersecurity Campaign

(1) STRONG AUTHENTICATION- (move from Passwords to PKI)…	**ACCESS**
(2) DEVICE HARDENING- (Configuration Mgt / SW Patching)…	**CONFIG MGT**
(3) REDUCE ATTACK SURFACE- (manage External Interfaces)…	**ATTACK SURFACE**
(4) CNDSP- (monitoring & diagnostics)…	**MONITORING**

Can we use any of these start points for other Scorecards ?

Assurance of - Mission --System --- Product / Component ---- Sub-Component



$

LEAST Capablabe adversaries to MOST

Min Rqts for Trusted Systems

Risk

Cybersecurity RMF & SCRM

Assured Services

Software (SwA) Assurance

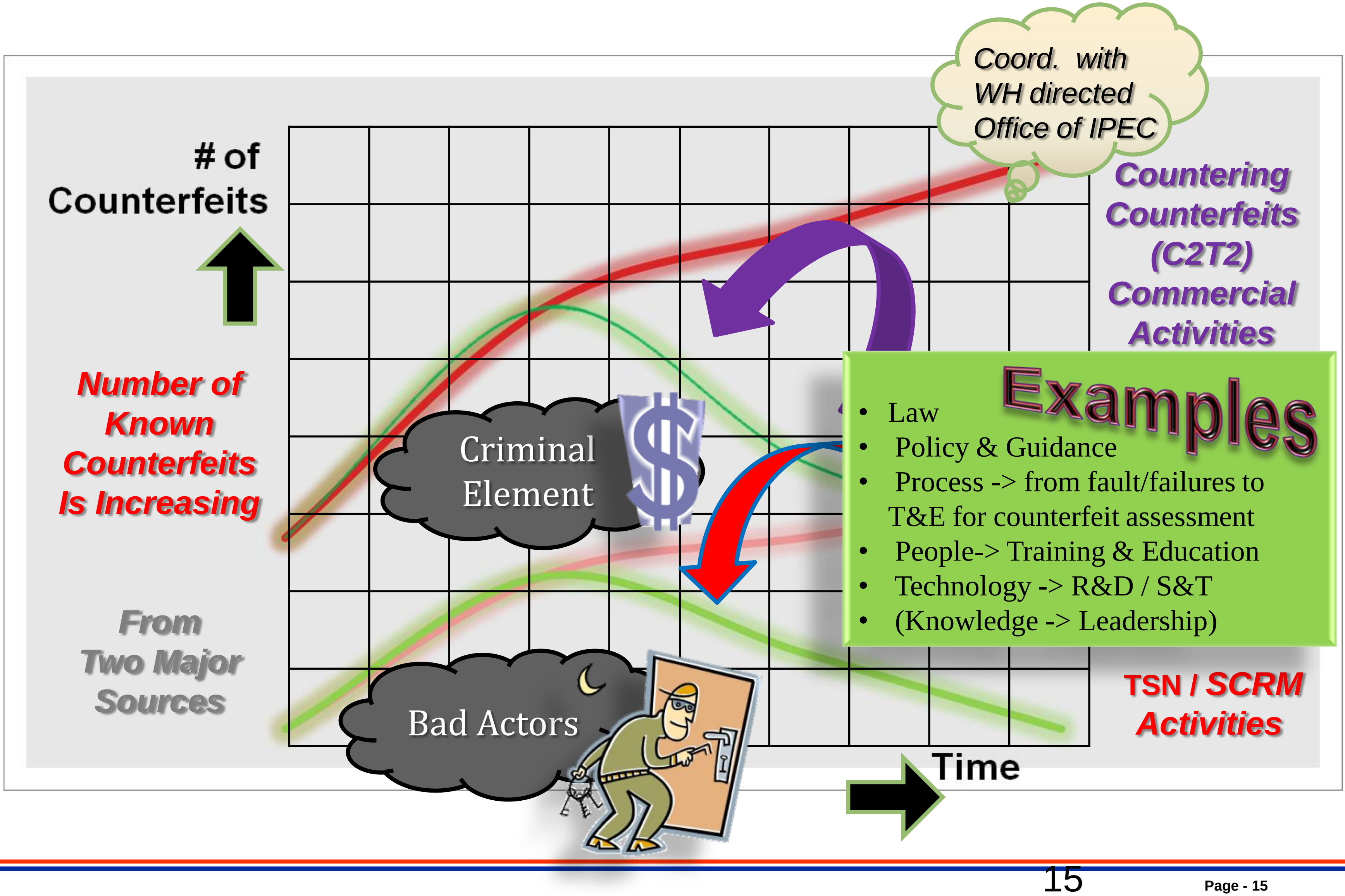
Counterfeit (HwA) Microelectronics

Minimum Requirements for All Systems

- ACCESS
- CONFIG MGT
- ATTACK SURFACE
- MONITORING

MOST Important Missions & Systems to LEAST

Countering Counterfeits Strategic Concept



Coord. with WH directed Office of IPEC

Countering Counterfeits (C2T2) Commercial Activities

Number of Known Counterfeits Is Increasing

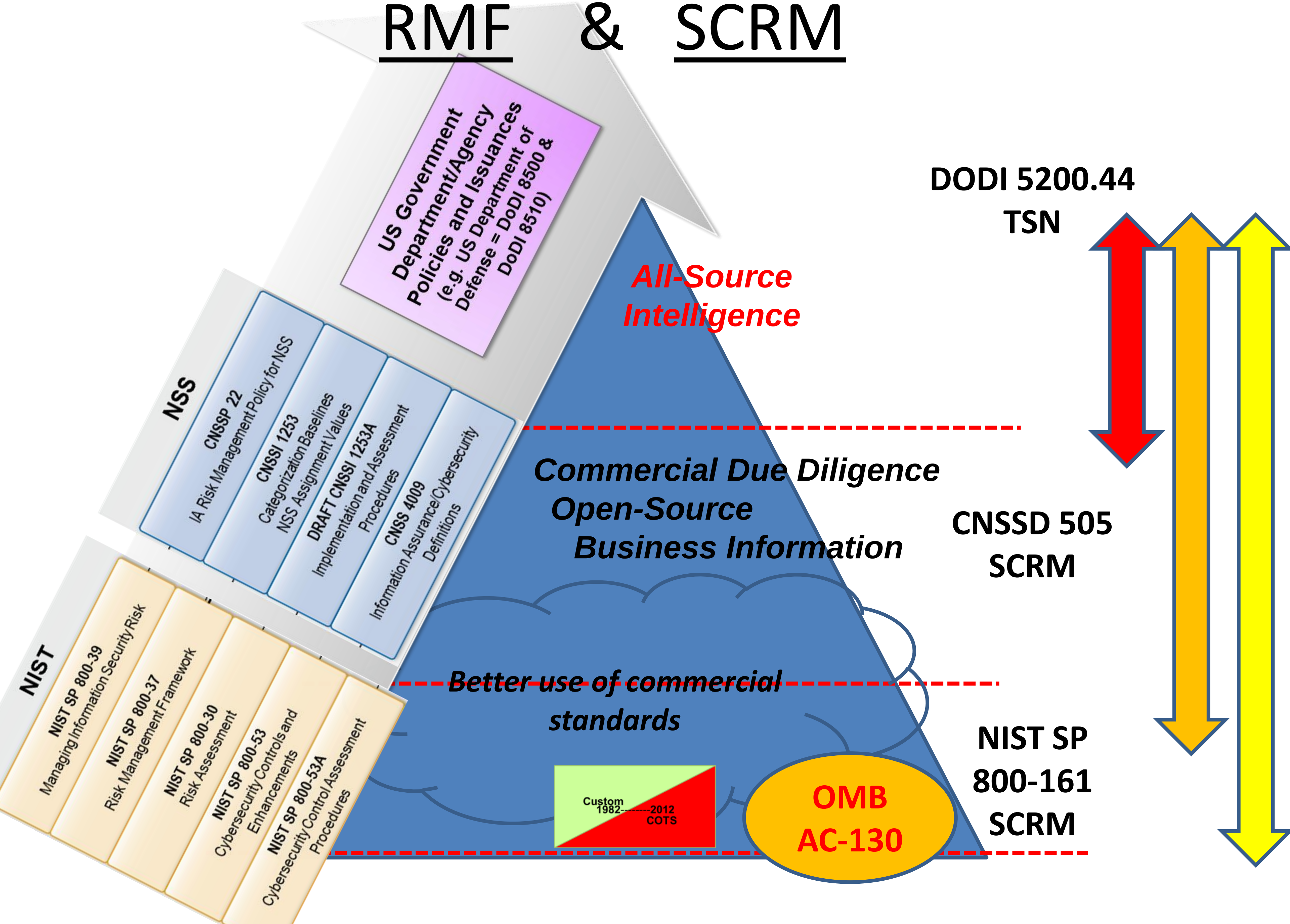
From Two Major Sources

TSN / SCRM Activities

Examples

- Law
- Policy & Guidance
- Process -> from fault/failures to T&E for counterfeit assessment
- People-> Training & Education
- Technology -> R&D / S&T
- (Knowledge -> Leadership)

RMF & SCRM



US Government Department/Agency Policies and Issuances (e.g. US Department of Defense = DoDI 8500 & DoDI 8510)
NSS
CNSSP 22
IA Risk Management Policy for NSS
CNSSI 1253
Categorization Baselines
NSS Assignment Values
DRAFT CNSSI 1253A
Implementation and Assessment Procedures
CNSS 4009
Information Assurance/Cybersecurity Definitions
NIST
NIST SP 800-39
Managing Information Security Risk
NIST SP 800-37
Risk Management Framework
NIST SP 800-30
Risk Assessment
NIST SP 800-53
Cybersecurity Controls and Enhancements
NIST SP 800-53A
Cybersecurity Control Assessment Procedures
All-Source Intelligence
Commercial Due Diligence
Open-Source
Business Information
Better use of commercial standards
Custom
1982---------2012
COTS
OMB AC-130
DODI 5200.44
TSN
CNSSD 505
SCRM
NIST SP 800-161
SCRM

Here is the stated purpose of OMB Circular A-130:

"This Circular establishes policy for the management of Federal information resources. OMB includes procedural and analytic guidelines for implementing specific aspects of these policies as appendices."

Here's the killer line to look for:

"Apply OMB policies and, for non-national security applications, NIST guidance to achieve adequate security commensurate with the level of risk and magnitude of harm."

And here's the hammer:

"Oversight: The Director of OMB will use information technology planning reviews, fiscal budget reviews, information collection budget reviews, management reviews, and such other measures as the Director deems necessary to evaluate the adequacy and efficiency of each agency's information resources management and compliance with this Circular."

Under FISMA all NIST FIPS documents are now required. The 800 series documents are also going to be used by OMB as "best practices" when conducting their audits. Implementing these NIST standards is going to be quite a lot of work for most agencies.

Thinking OUTLOUD ?

(1) We need to establish some big cut lines / levels of assurance !
How do we consider a System-of-Systems approach to these levels?
How do we address Mission / System / Component / sub-component ?

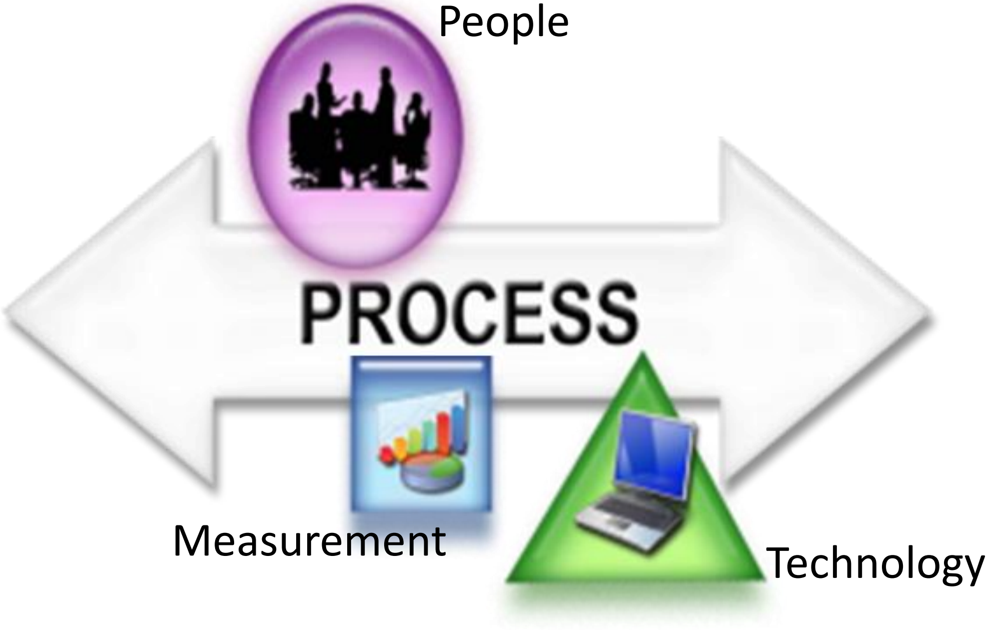
(2) What is the role of Basic Cyber(hygiene) Reqts?
What is balance of keeping up w/ innovation & security (CIO / CISO)?

(3) How do we better consider / use COTS products?
How do we better exploit reciprocity? (test once)
How do we better use "WHITELISTS" / pre-approvals ?
-we do NOT BLACKLIST !

(4) What is the role of:
-TSN Reqts
-Common Criteria (NIAP) / PP-SRGs
-DISA STIGS
-FIPS & FISMA reqts / certs
-UC Approved Products List
-DLA / MDA Approved Supplier Lists
-GSA schedule

BACK-UP

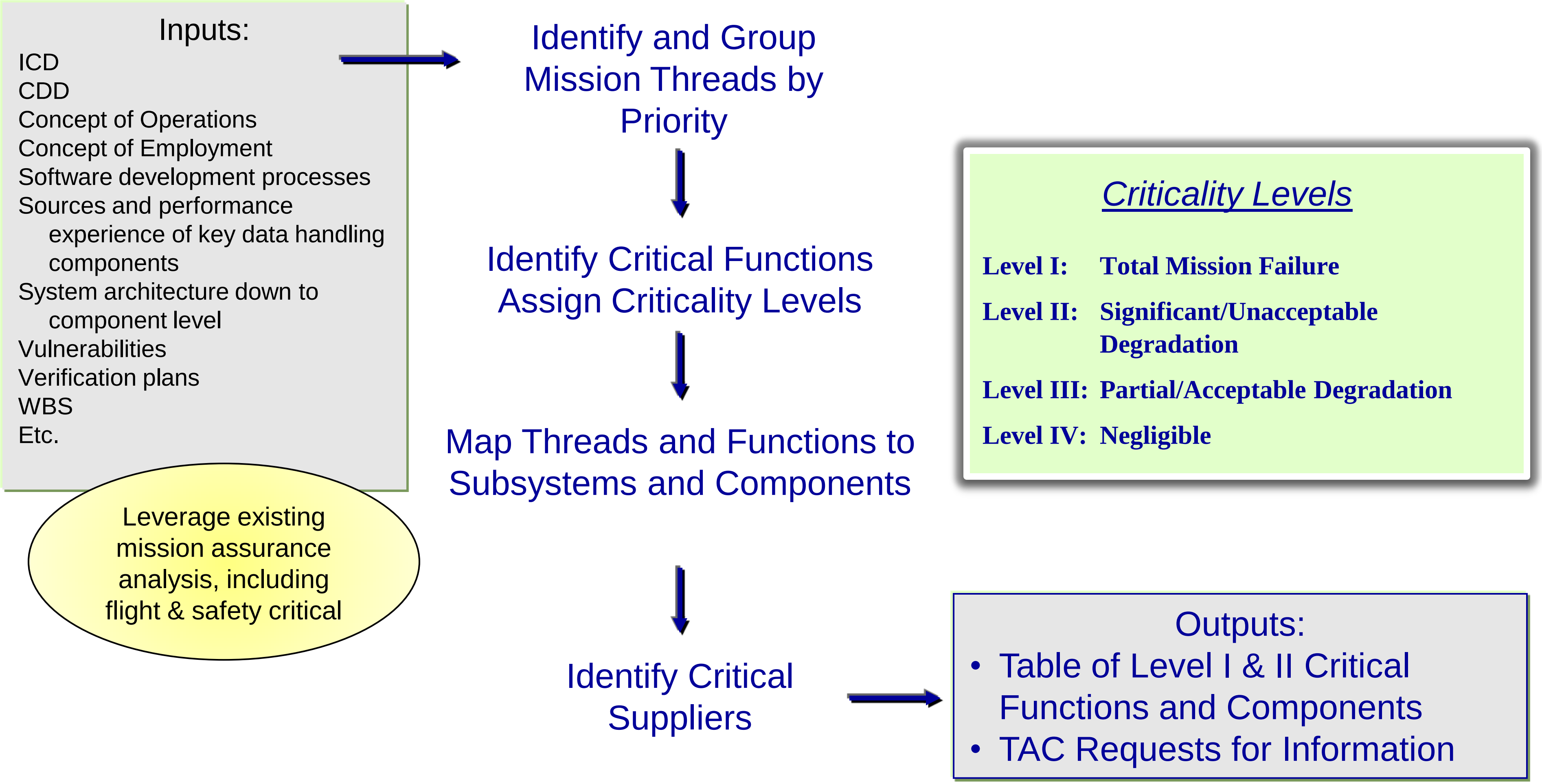
There is a need to develop the **Science of Cybersecurity**



We need to better understand how to measure cybersecurity / cyber risk?

Criticality Analysis Methodology

Criticality Analysis



Inputs:

ICD
CDD
Concept of Operations
Concept of Employment
Software development processes
Sources and performance experience of key data handling components
System architecture down to component level
Vulnerabilities
Verification plans
WBS
Etc.

Leverage existing mission assurance analysis, including flight & safety critical

Identify and Group Mission Threads by Priority

Identify Critical Functions
Assign Criticality Levels

Map Threads and Functions to Subsystems and Components

Identify Critical Suppliers

Criticality Levels

Level I:	**Total Mission Failure**
Level II:	**Significant/Unacceptable Degradation**
Level III:	**Partial/Acceptable Degradation**
Level IV:	**Negligible**

Outputs:

- Table of Level I & II Critical Functions and Components
- TAC Requests for Information

Risk Assessment Methodology

Input Analysis Results:

Criticality Analysis Results

Mission	Critical Functions	Logic-Bearing Components (HW, SW, Firmware)	System Impact (I, II, III, IV)	Rationale
Mission 1	CF 1	Processor X	II	Redundancy
	CF 2	SW Module Y	I	Performance
Mission 2	CF 3	SW Algorithm A	II	Accuracy
	CF 4	FPGA 123	I	Performance

Vulnerability Assessment Results

Critical Components (HW, SW, Firmware)	Identified Vulnerabilities	Exploit-ability	System Impact (I, II, III, IV)	Exposure
Processor X	Vulnerability 1 Vulnerability 4	Low Medium	II	Low Low
SW Module Y	Vulnerability 1 Vulnerability 2 Vulnerability 3 Vulnerability 6	High Low Medium High	I	High Low Medium Low
SW Algorithm A	None	Very Low	II	Very Low
FPGA 123	Vulnerability 1 Vulnerability 23	Low Low	I	High High

Threat Analysis Results

Supplier	Critical Components (HW, SW, Firmware)	TAC Findings
Supplier 1	Processor X	Potential Foreign Influence
	FPGA 123	Potential Foreign Influence
Supplier 2	SW Algorithm A	Cleared Personnel
	SW Module Y	Cleared Personnel

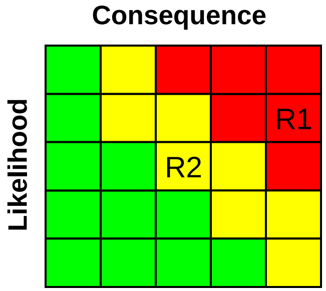
Risk Mitigation and Countermeasure Options

Risk Assessment

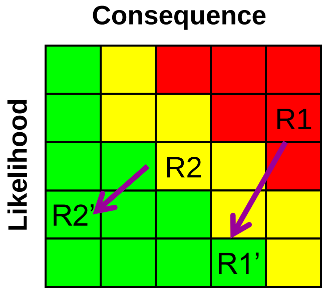
Consequence of Losing Mission Capability
Very High
High
Moderate
Low
Very Low

Likelihood of Losing Mission Capability
Near Certainty (VH)
Highly Likely (H)
Likely (M)
Low Likelihood (L)
Not Likely (VL)

Initial Risk Posture



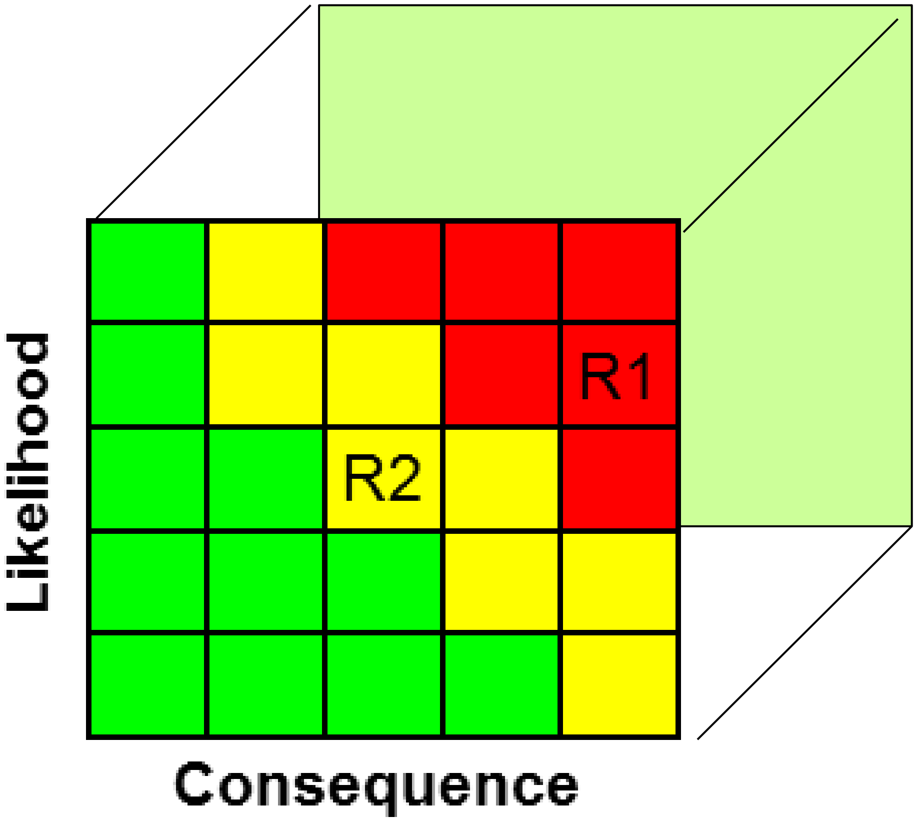
Risk Mitigation Decisions



M&S / SE Challenge

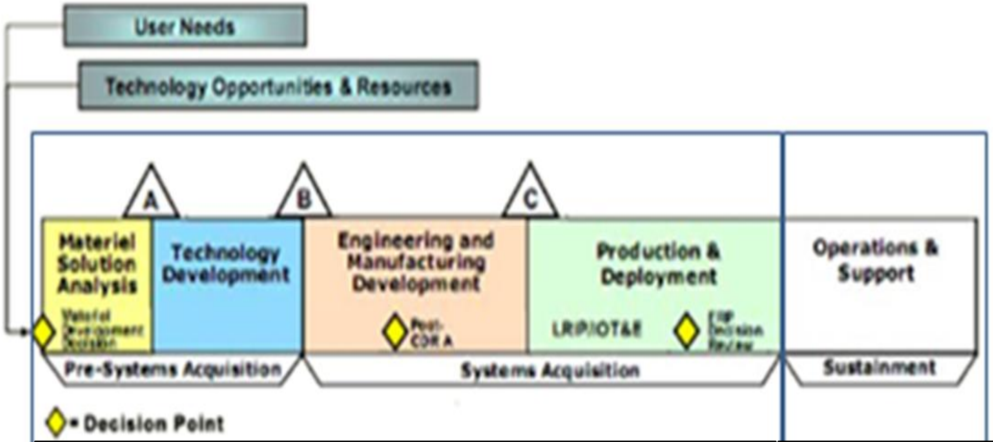
Can we put some science into measuring & trading risks ?

- Confidentiality
- Integrity
- Availability



🟩	🟨	🟥	🟥	🟥
🟩	🟨	🟨	🟥	🟥 R1
🟩	🟩	🟨 R2	🟨	🟥
🟩	🟩	🟩	🟨	🟨
🟩	🟩	🟩	🟩	🟨

DoD 5000 Defense Acquisition System



REQTS

SS-KPP (CSE)

Dev & Acq

Weapon Systems / (PIT)

Information Systems (IS)

O&S

Weapon Systems / (PIT)

Information Systems (IS)