# Globalization is **Good**, *but...*

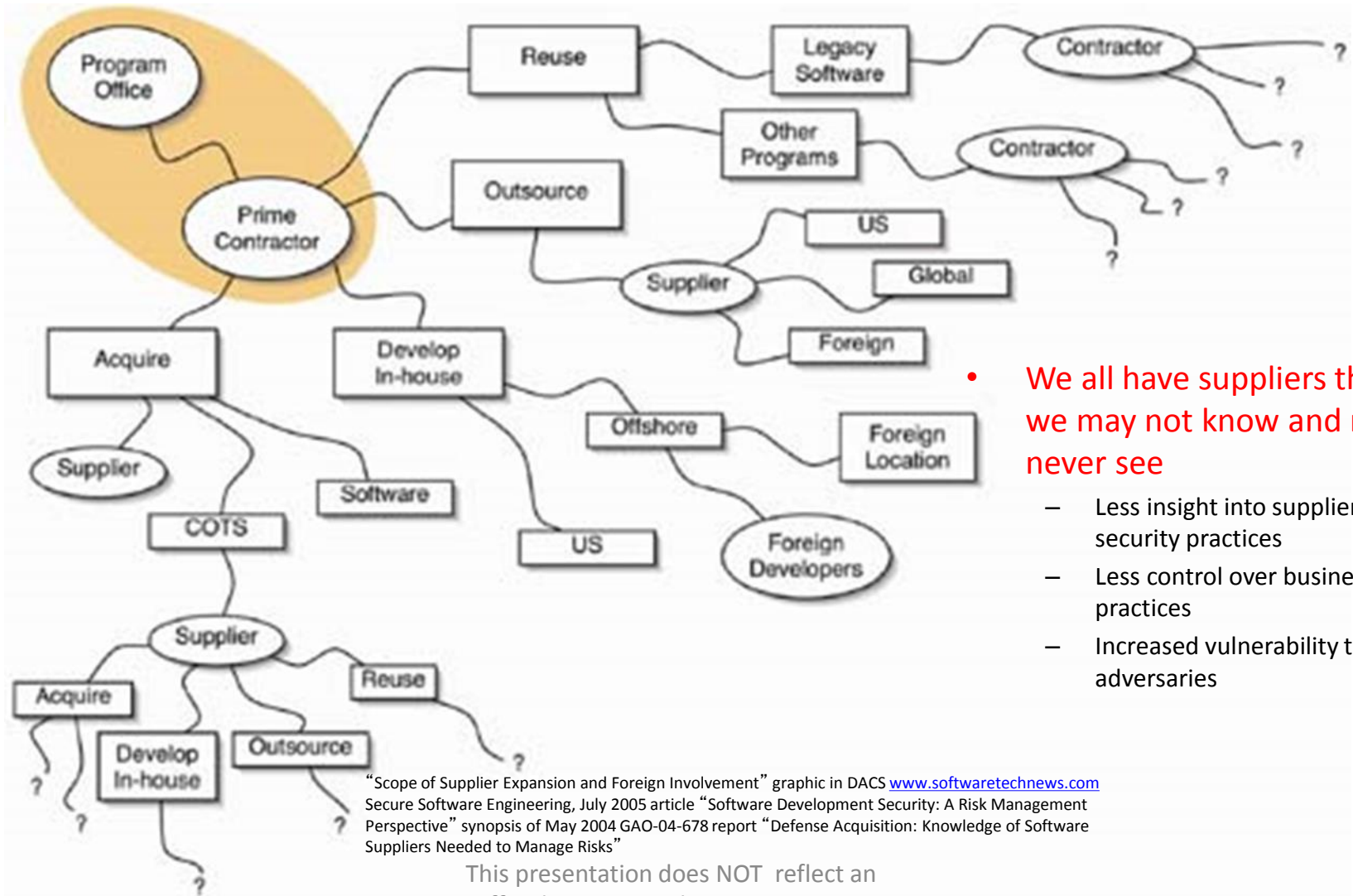> **"*Your* technology solution might be *my* security challenge."**

***Don Davidson***
**Deputy Director, Cybersecurity (CS) Lifecycle**
**Risk Management & CS / Acquisition Integration**
**In the Office of the Deputy DoD-CIO for Cybersecurity (CS)**

*Donald.R.Davidson4.civ@mail.mil*

This presentation does NOT reflect an
official US National or DoD position.

# Globalization is good, but it brings challenges



- **We all have suppliers that we may not know and may never see**
  - Less insight into suppliers' security practices
  - Less control over business practices
  - Increased vulnerability to adversaries

"Scope of Supplier Expansion and Foreign Involvement" graphic in DACS www.softwaretechnews.com Secure Software Engineering, July 2005 article "Software Development Security: A Risk Management Perspective" synopsis of May 2004 GAO-04-678 report "Defense Acquisition: Knowledge of Software Suppliers Needed to Manage Risks"

This presentation does NOT reflect an official US National or DoD position.
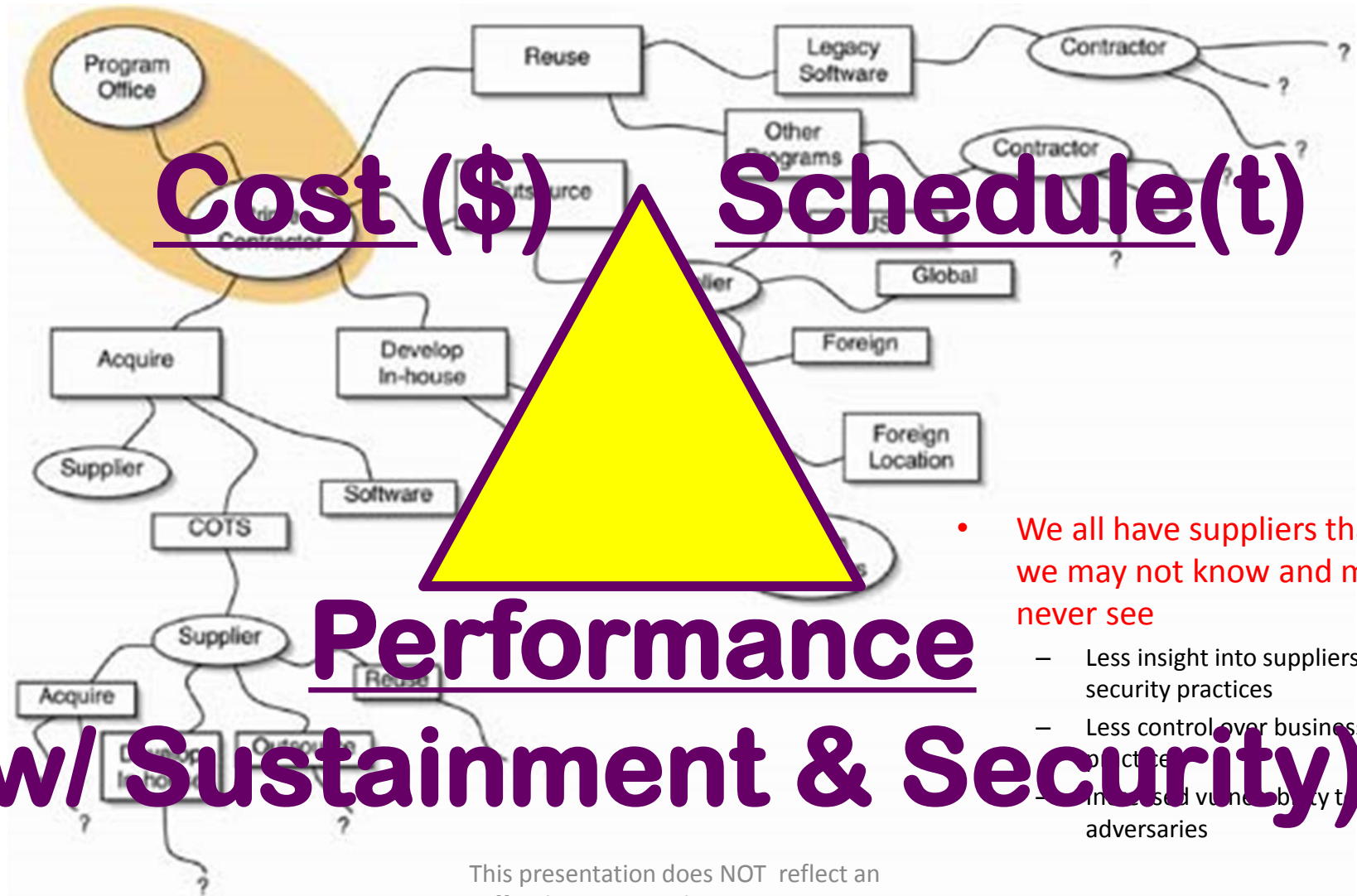
# Globalization is good,
## but it brings challenges
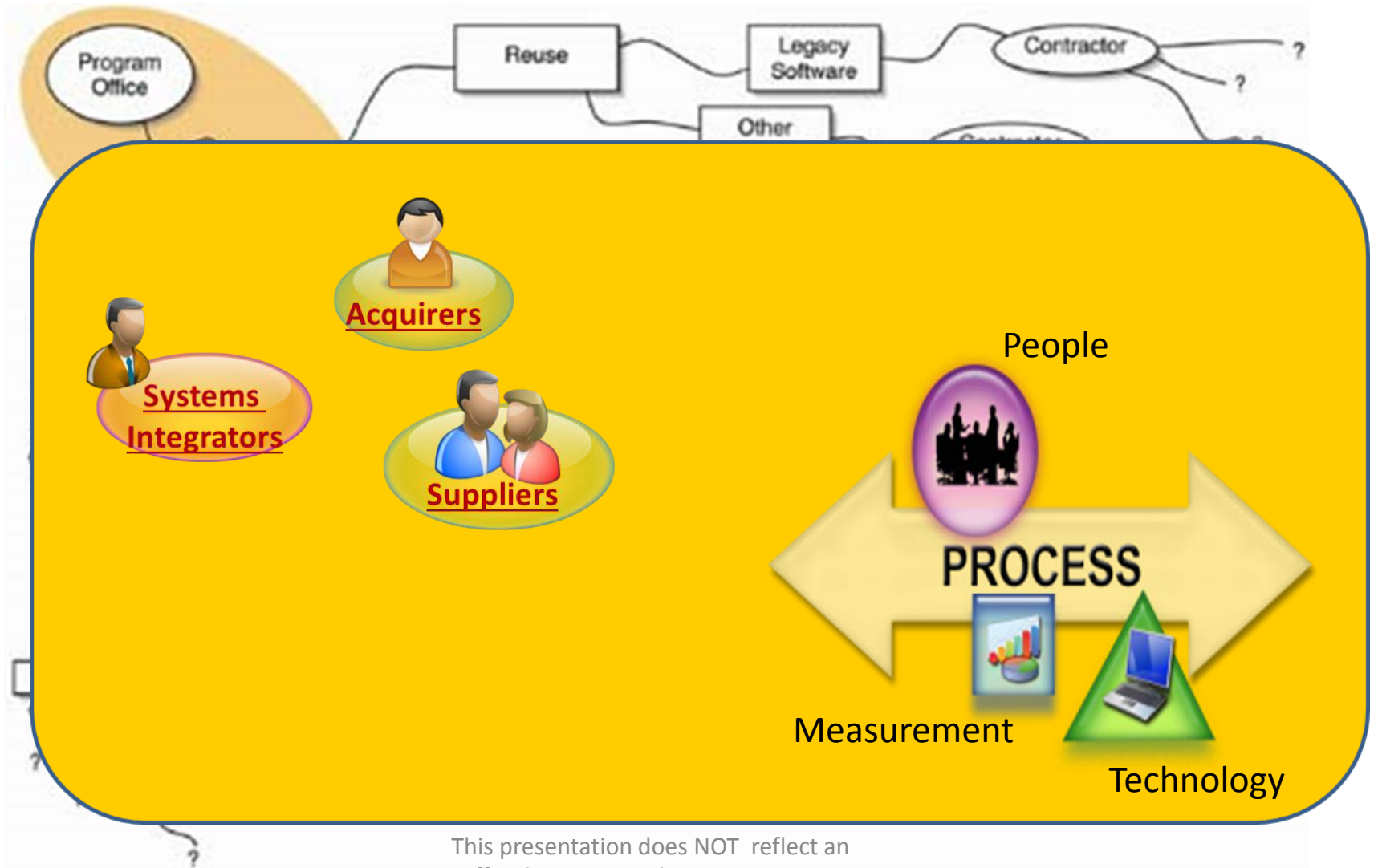


**Cost ($)** **Schedule(t)**

**Performance**
**( w/ Sustainment & Security)**

- We all have suppliers that we may not know and may never see
  - Less insight into suppliers' security practices
  - Less control over business practices
  - Increased vulnerability to adversaries

# Globalization is good,
# but it brings challenges

Not only do we have an

<span style="color:red">increasingly</span>

**Global-Interdependent Supply Chain,**

we also have a world of

Capabilities, that are

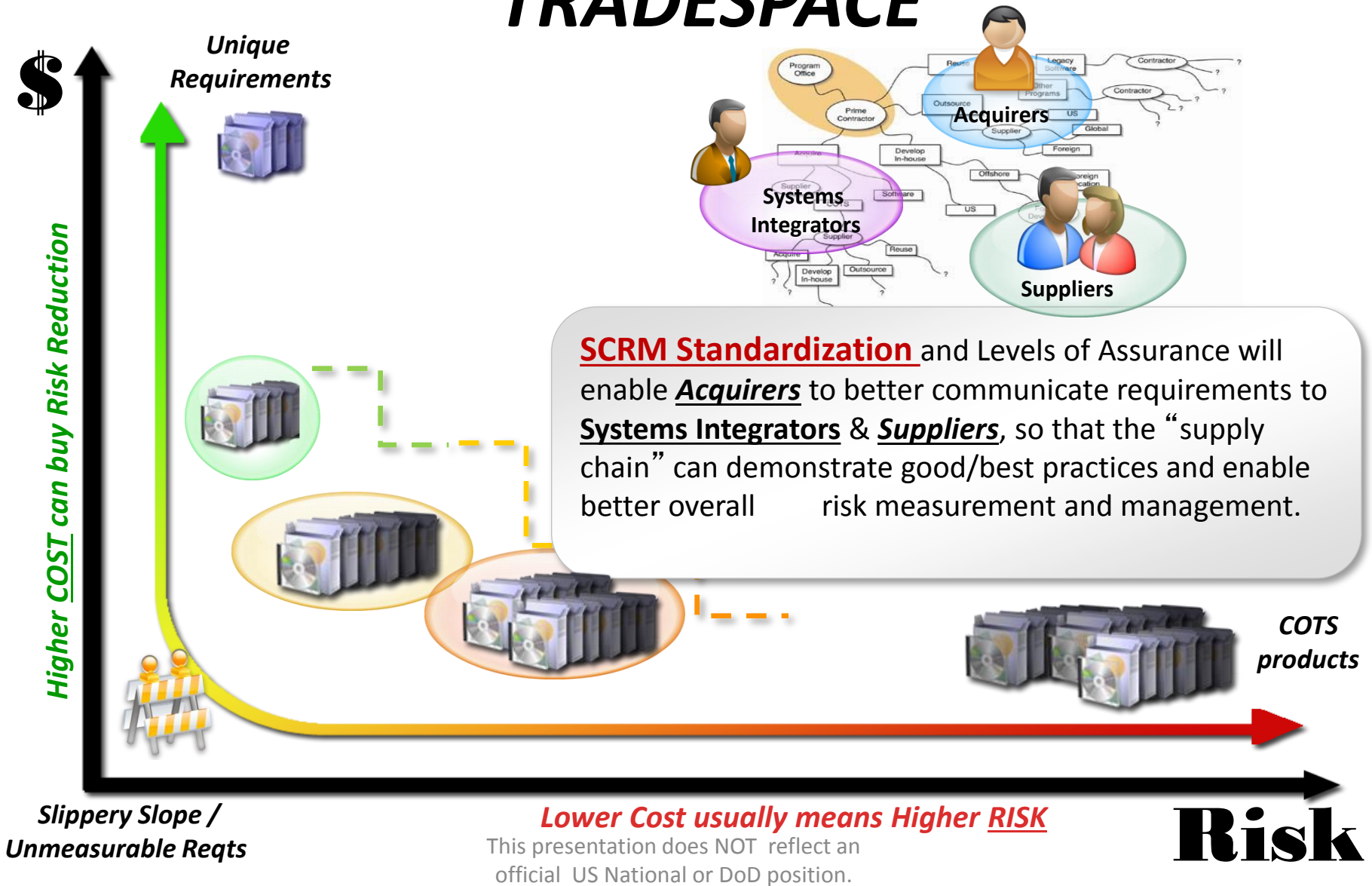<span style="color:red">increasingly</span>

**Dependent on Globally-Sourced**

**Commercial-Off-The-Shelf (COTS)**
**Information Communications**
**Technology (ICT)**

# Product Assurance
## *TRADESPACE*

**$**

*Higher COST can buy Risk Reduction*

**Unique Requirements**

**Acquirers**

**Systems Integrators**

**Suppliers**

**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.

**COTS products**

*Slippery Slope / Unmeasurable Reqts*

*Lower Cost usually means Higher RISK*
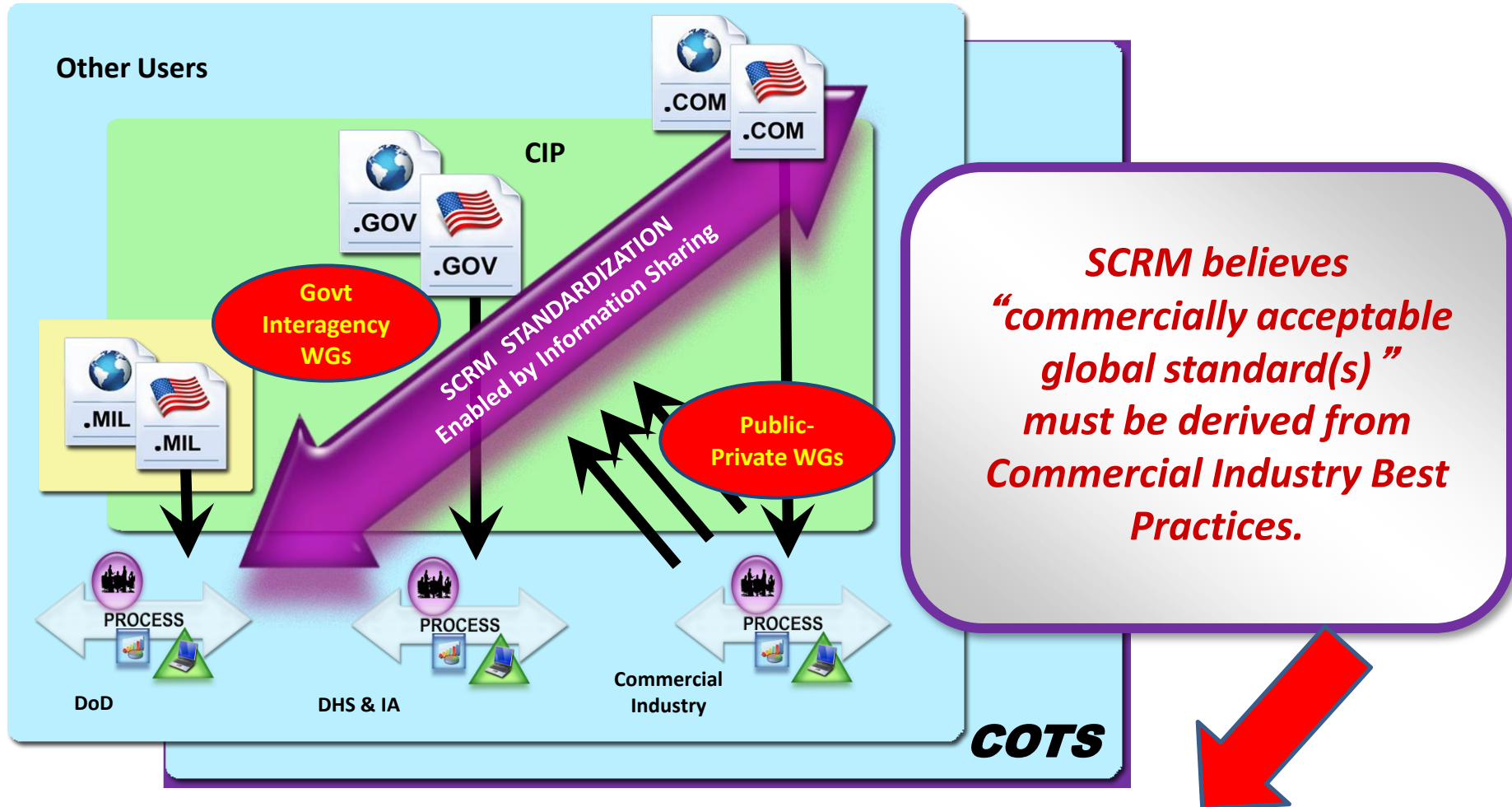
This presentation does NOT reflect an official US National or DoD position.

# Risk

# Supply Chain Risk Management (SCRM)
## SCRM has a Landscape of activities

*US has vital interest in the global supply chain.*



Other Users

CIP

.COM

.GOV

.MIL

**Govt Interagency WGs**

SCRM STANDARDIZATION
Enabled by Information Sharing

**Public-Private WGs**

PROCESS

DoD

DHS & IA

Commercial Industry

COTS

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

## SCRM Standardization Requires Public-Private Collaborative Effort

# END STATE is delivery of a YACHT

**Delivering what:**

An **85' custom-built motor yacht** complete with 4 state rooms, a state-of-the-art galley, GPS System and radar for navigation, twin supercharged diesel engines, etc.

**$7,474,793.00**

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Event to deliver: Champagne, chocolate covered strawberries with cream and music dockside for the excited 'soon to be owner' and a small group of his friends**

**$1500.00**

# What is critical in a given process?



This presentation does NOT reflect an
official US National or DoD position.

**What is critical in a given process?**

**The act of delivering:**

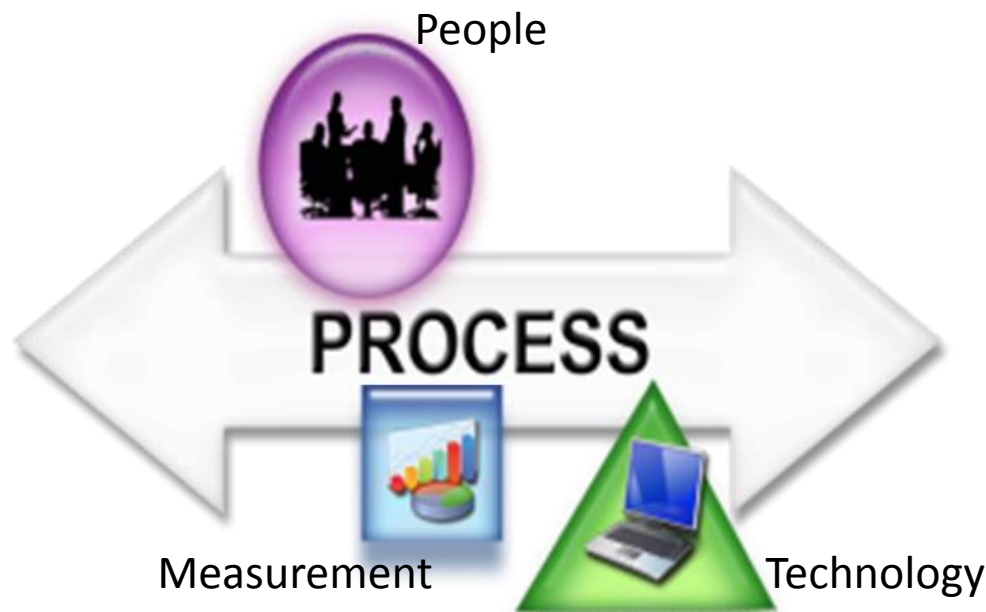**Two corporate representatives, crane, and rigging $2,500.00 / hour minimum…**

**complete with a**

**"faulty" $25.00 dollar turnbuckle.**

This presentation does NOT reflect an
official US National or DoD position.

# What is critical in a given process?

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



People

PROCESS

Measurement          Technology

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

**"We Cannot Blindly Reap the Benefits of a Globalized ICT Supply Chain!" CROSSTALK Magazine 2013**

http://www.crosstalkonline.org/storage/issue-archives/2013/201303/201303-0-Issue.pdf

**Software & Supply Chain Assurance (SSCA) Forum(s)**

www.gsa.gov/portal/content/220411

https://buildsecurityin.us-cert.gov/resources/websites

**ISO/IEC 27036-1:2014**
**Information technology -- Security techniques -- Information security for supplier relationships -- Part 1: Overview and concepts**

www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59648