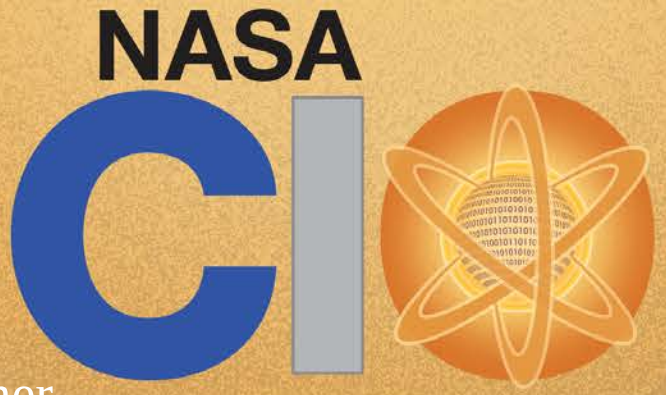
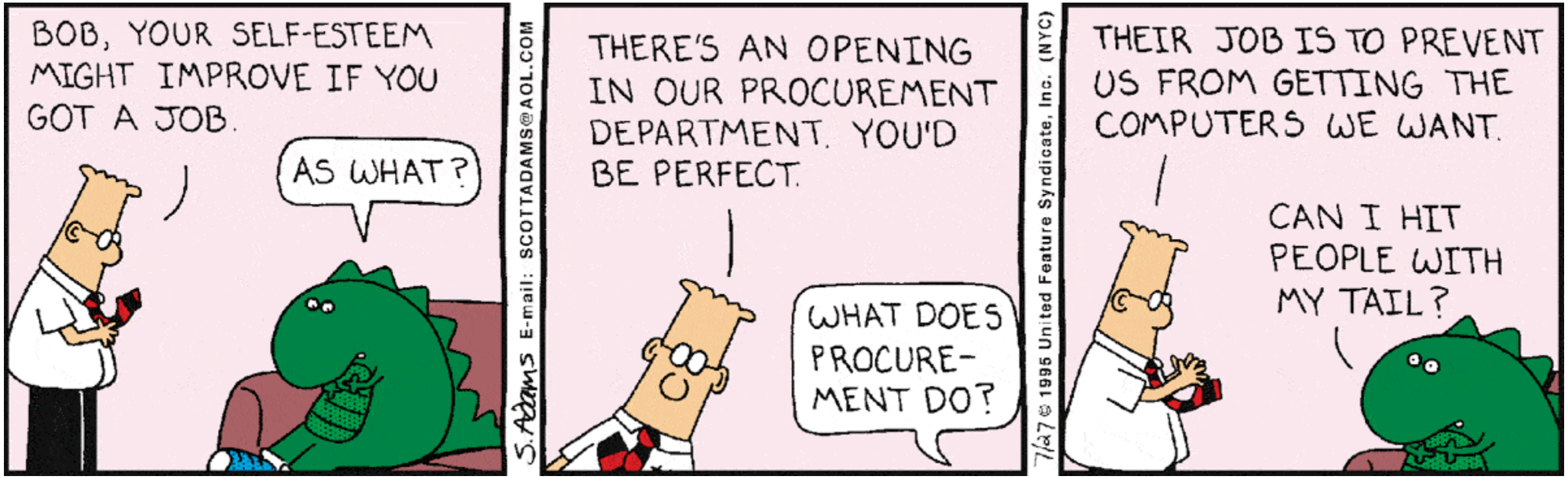
National Aeronautics and Space Administration

NASA's Information & Communications Technology (ICT) Supply Chain Risk Management (SCRM)



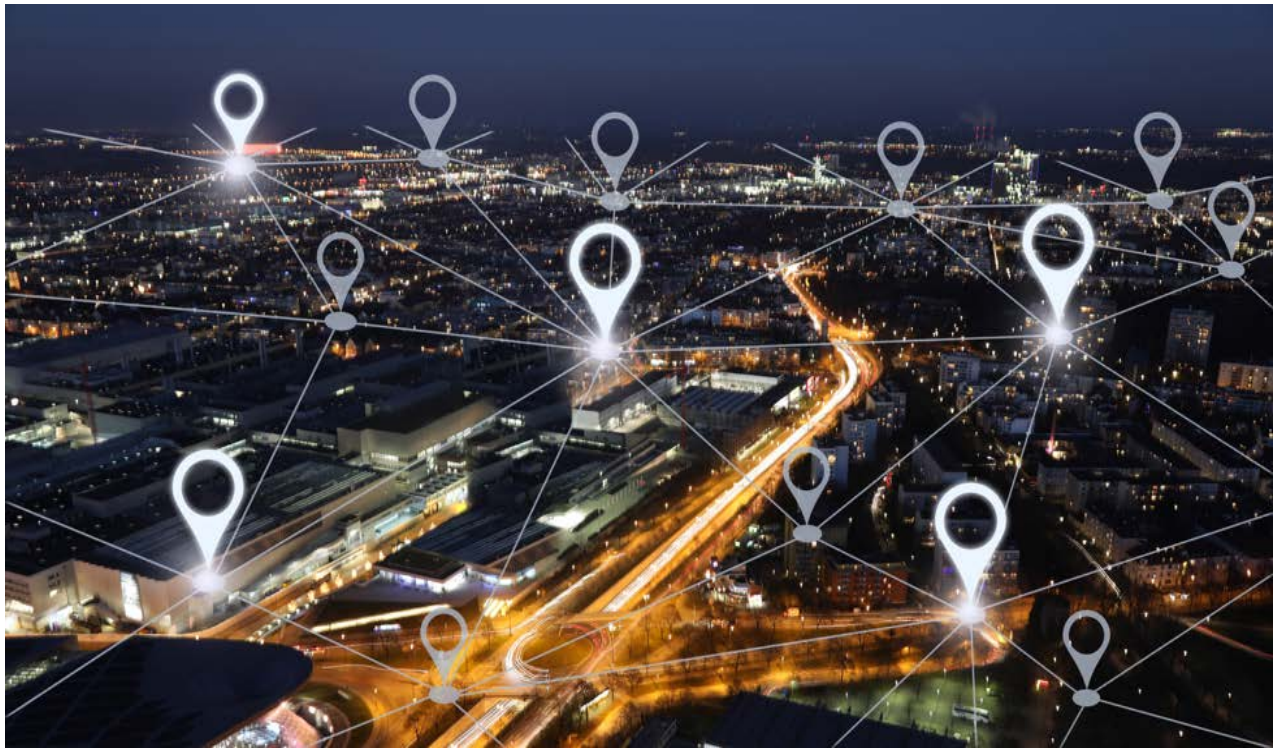
Kanitra Tyler, NASA SCRM Service Owner
SSCA – 05/09/2019

Let's Work Together



The Three P's of NASA SCRM

- Provenance
  - Blockchains - Transparent, Traceable, and Tamper-Proof Supply Chain Data
  - Each link in the Supply Chain being able to trust the link before and after it
- Pedigree
  - Tracking of manufactured products through the distribution channels prevents counterfeiting and ensures safety and security of products
- Position
  - Innovation and efficiency in contracting management with provider optimization and redundancy



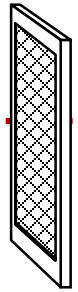
Current Process

NASA's Office of the Chief Information Officer (OCIO) Request for Investigation (RFI) Process

Center POC
Initiates procurement request for Agency missions

Center OCIO
Conducts internal review to verify if items has been previously assessed and cleared by OCIO. If yes, request if forwarded to the Office of Procurement for processing. If not, a RFI is forwarded to Center SCRM Analyst for further review

Office of Procurement
Initiates purchase request of assessed and cleared item.



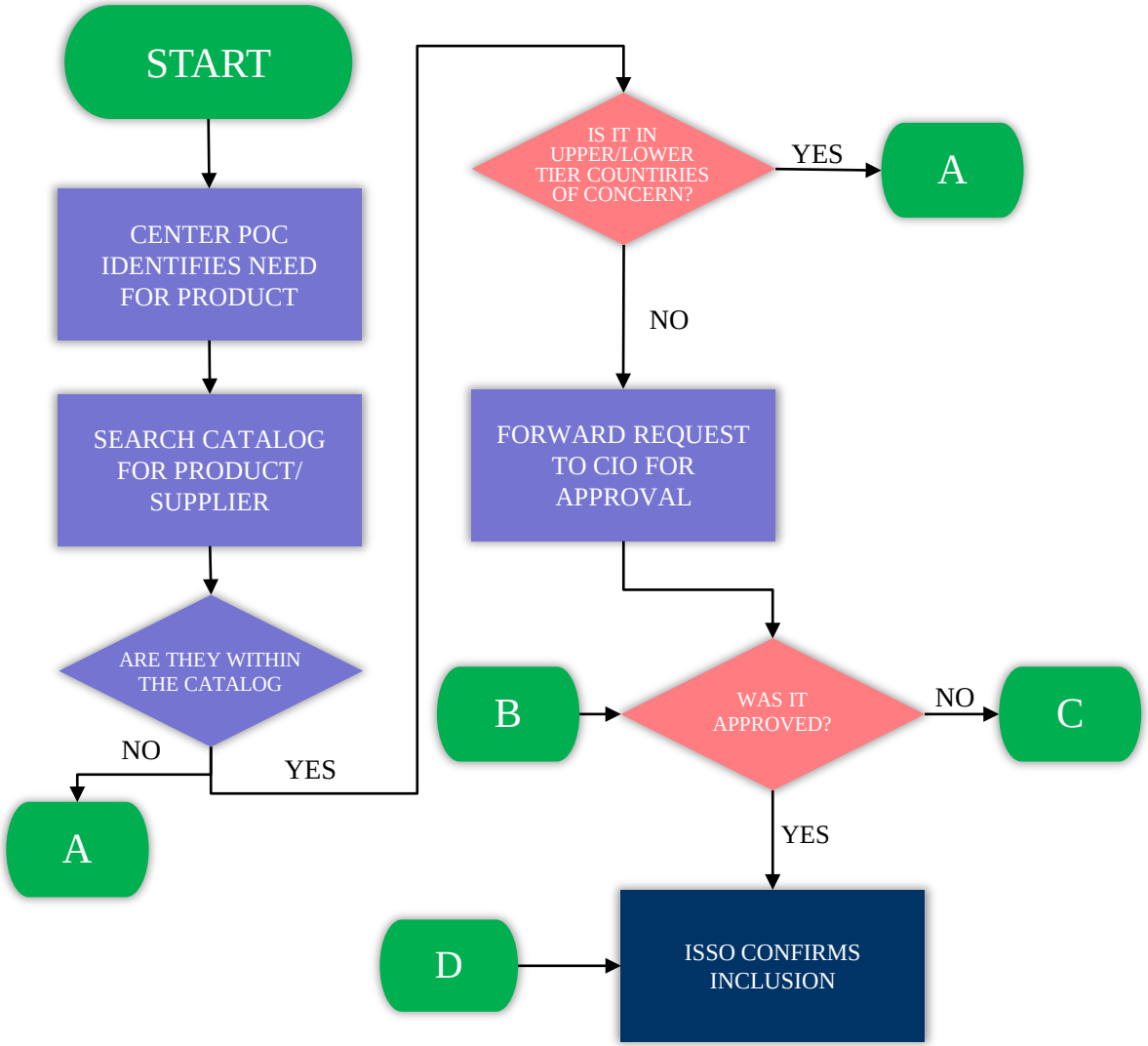
Center SCRM POC
Analyst interfaces between Centers and the OCIO Office

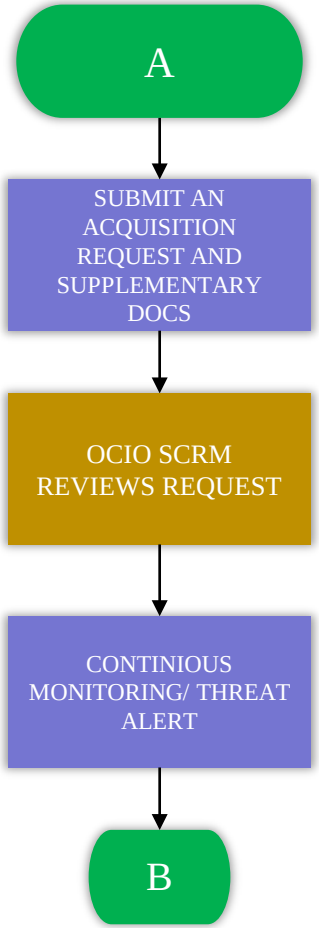
NASA OCIO SCRM Analyst
OCIO Analyst Conducts Risk Assessment

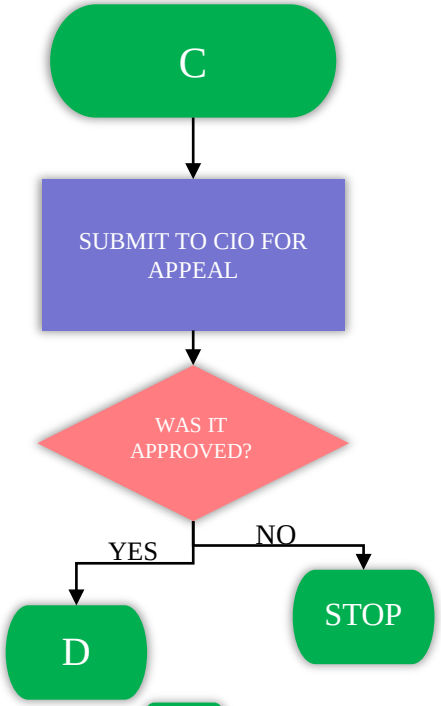
NASA OCIO
Makes final determination to clear item based on assessment. If cleared, item is added to the ACL and Center is notified to proceed with purchase. If not cleared, Center is notified of final decision.

External Collaboration
Consults with Federal Bureau of Investigations, Department of Defense, National Institute of Standards and Technology, NASA's Counterintelligence Office and other NASA cybersecurity partners to understand threat vectors, system and/or component acquisition risk to the NASA environment and develop risk mitigation strategies.

Future Process







Not in Catalog A

Send to CIO B

Appeal C

Send to ISSO D

OCIO

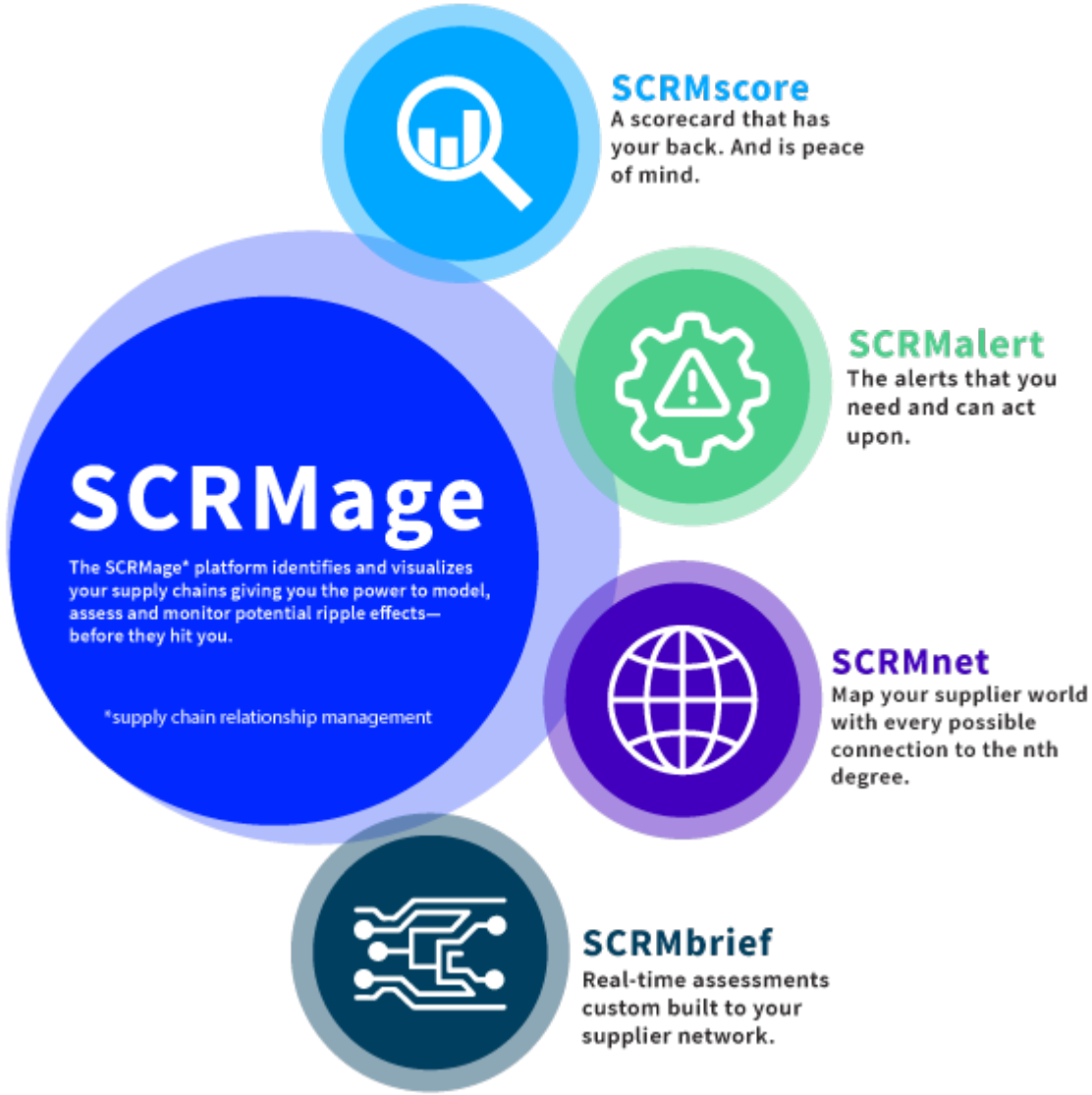
Requester

CIO

Start/Finish

ISSO

Introducing SCRMage



https://youtu.be/pG2r0WZIXi8

SCRM Service Overview

Map	Assess	Score	Monitor
Connections & Interactions	Knowledge, Risks & Vulnerabilities	Quantified Risk Benchmarks	Emerging Risks & Vulnerabilities

The Interos Platform, SCRMage, allows NASA to:

- Understand the complex connections and dependencies across your ecosystem
- Increase end-to-end transparency and knowledge of your multi-tier ecosystem
- Answer complex risk and resiliency questions impacting suppliers across your ecosystem
- Continuous discovery of indicators of risks for individual suppliers and your supply chains
- Eco-system Maps, Supplier Insights, Risk Scores, and Continuous Monitoring

Challenges

1. Distinguishing ICT vs non-ICT products and services
2. Inefficient and inconsistent implementation of ICT SCRM across the Federal Government
3. Procurement regulations, processes and integration
   a. Classified information is not readily actionable by Agencies and Procurement Officials
   b. Federal Procurement Schedules can't readily reflect risks/changes as identified
4. Federal Bureau of Investigation (FBI)
5. Limited skillsets and resources
6. Breaking Cost, Schedule, Performance Barriers

Proposed Supply Chain Risk Management Process for USG Civil and NSS Space Program

Lori Gordon
Civil Systems Project Lead
The Aerospace Corporation

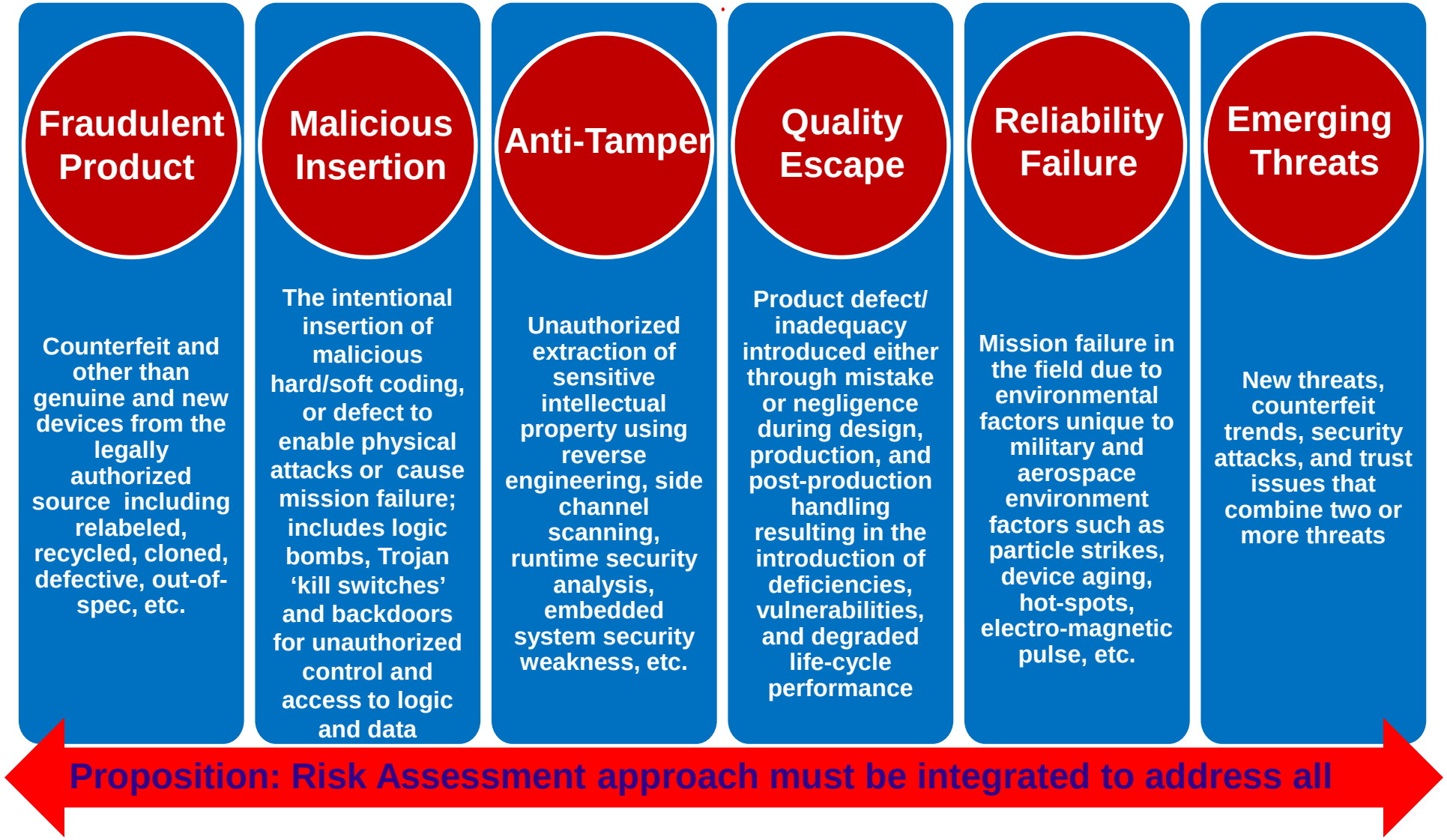
SSCA – 09 May 2019

Background

Why the emphasis on Supply Chain Risk Management

- Proliferation of counterfeit, fraudulent and malicious electronic parts and materials entering through supply chains
  - *Evidence: Increases in GIDEP reporting over the past 10 years*
    - More seizures by DHS CBP and ICE of counterfeit products entering the US
  - *Opportunity: Increasing dependency on non-authorized / non-franchised suppliers (i.e., brokers)*
  - *Foreign adversaries increased capability for tampering with and inserting malicious codes into advanced microelectronics*
- Greater dependency on foreign and non-trusted sources of supply for electronic parts and advanced technology nodes
  - *Global supply chain – many foreign companies are an integral part of the supply chain; i.e., design centers, wafer fabs, packaging and testing facilities*
    - Foreign suppliers are 2 – 3 generations ahead in technology development
- Cyber Attacks and Exfiltration / Theft of US Industrial Base Intellectual Property
- Impacts
  - *What is known: discovered through screening / testing*
  - *What is unknown: cost, reliability, susceptibility to foreign intrusion*

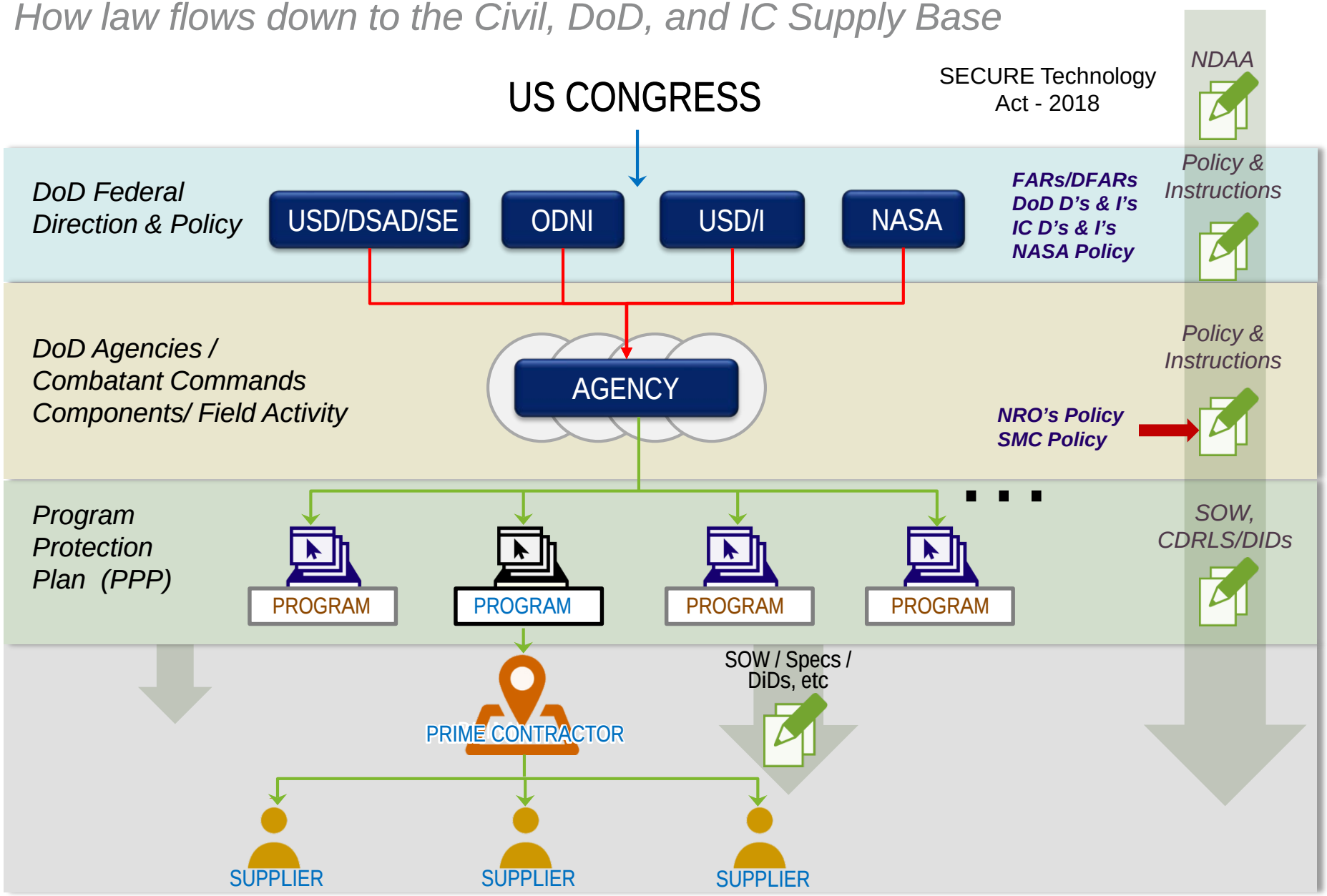
Many Supply Chain Risks to Consider



Slide courtesy DoD/AT&L(DSAD/SE)

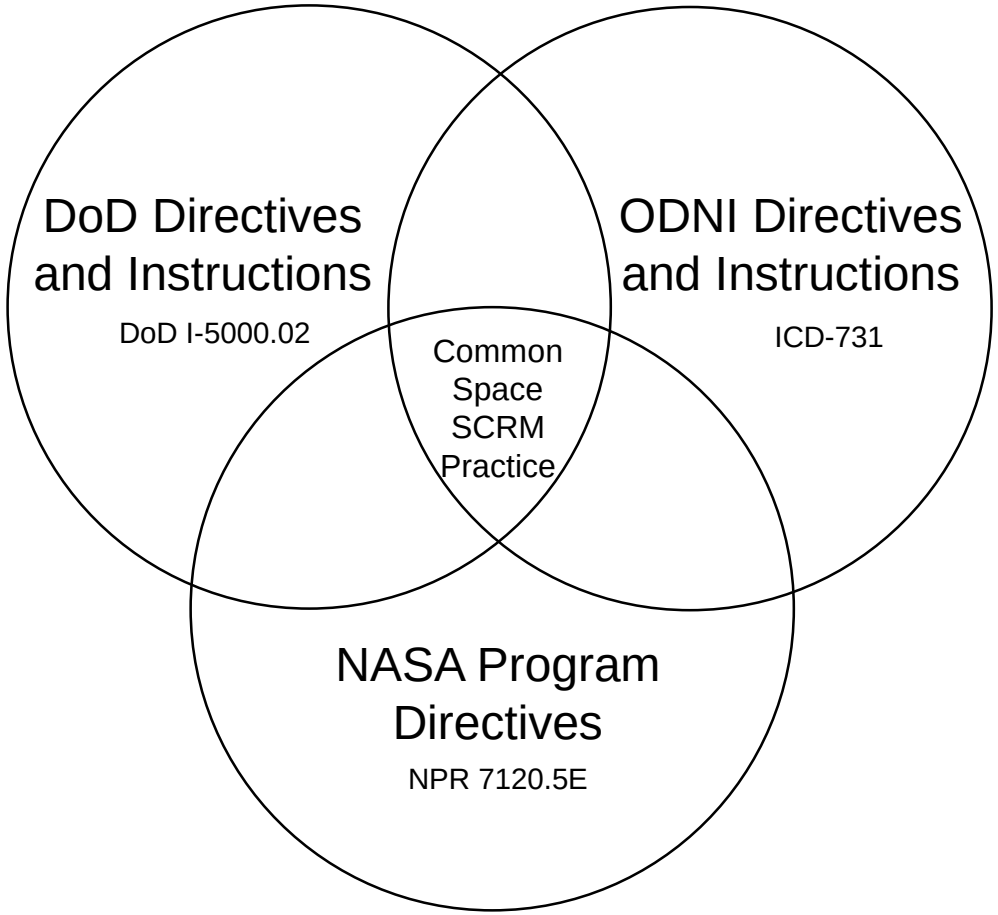
Congress to Contracts

How law flows down to the Civil, DoD, and IC Supply Base



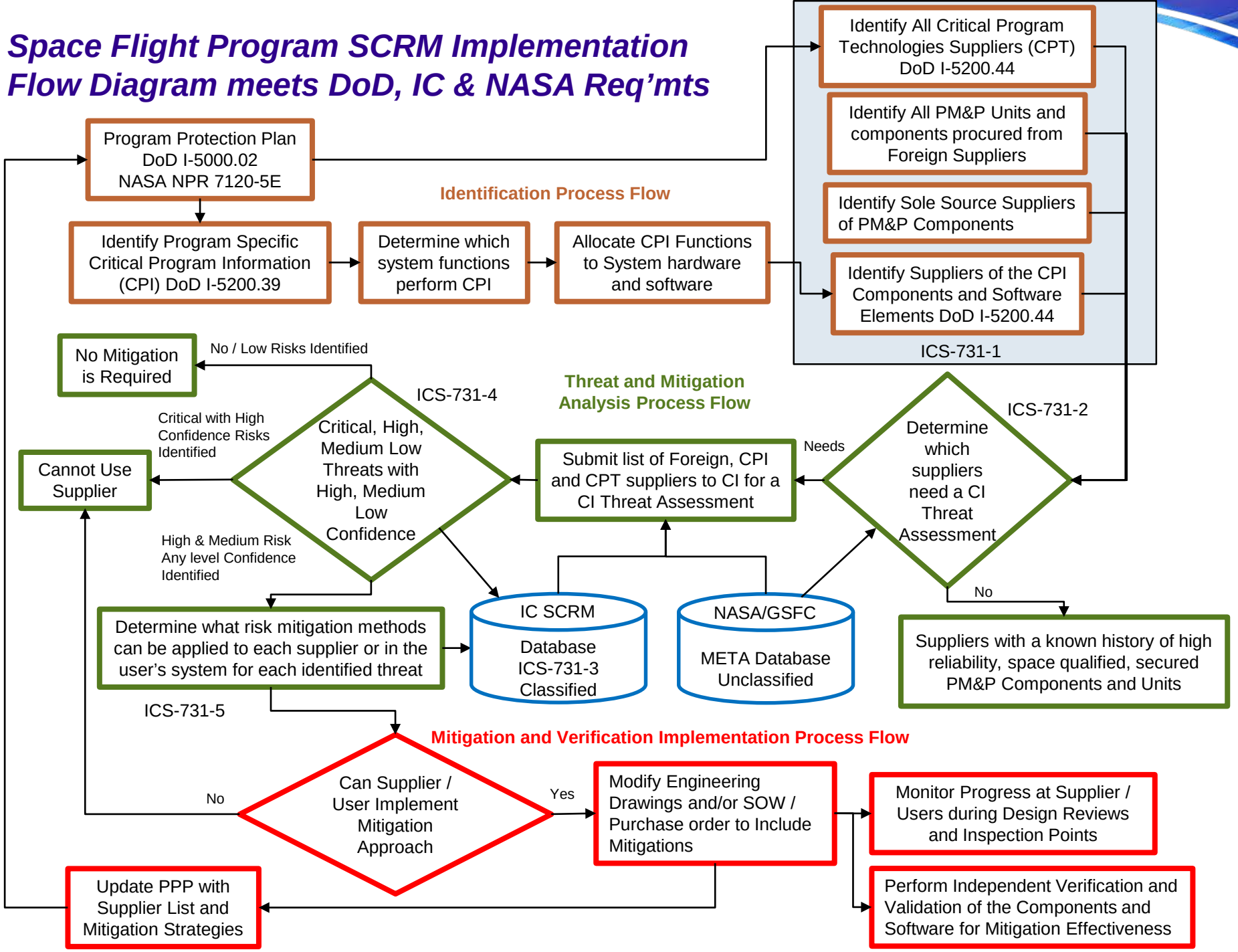
DoD, ODNI, NASA SCRM Requirements

Process needs to include multiple supply chain threat vectors



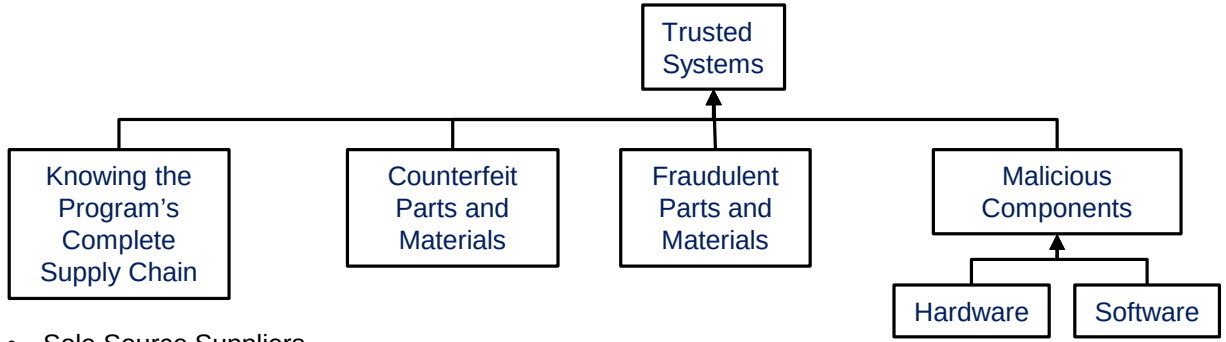
Develop a common SCRM process that meets the INTENT of Congressional, DoD, ODNI, and NASA requirements

Space Flight Program SCRM Implementation Flow Diagram meets DoD, IC & NASA Req'mts



Aerospace's– Proactive Actions (1)

Space Quality Improvement Council and Mission Assurance Improvement Workshop



Trusted Systems can be flight (space) and ground (operational) systems

- SCRM Implementation is different for these systems and service contract providers
- Apply Mission Assurance / SCRM standards to flight program contracts
- Aerospace is working to define Mission Assurance / SCRM standards (TORs) for ground systems and service contract providers
  - *Ground systems SCRM mainly focuses on Cyber SCRM practices such as NIST SP 800-161*

These TORs will describe methodologies for SCRM Implementation that meet the intent of the DoD, IC and NASA requirements documents and philosophy

Aerospace's– Proactive Actions (2)

SCRM Training Program for Program Offices and Contractors

- SCRM Training Class is a spin off from the PM&P/MA PROPEL Class
- Developed with assistance / inputs from
  - DoD/AT&L OSD DSAD/SE
  - NSWC – Crane
  - Institute for Defense Analysis (IDA)
  - FBI / NRO Office of Counterintelligence
  - Aerospace SMEs
- Provides real world examples of
  - Threats / Occurrences in USG Systems
  - Impacts to Programs
  - Requirements flow down
  - Microelectronics Trust Requirements
  - Best SCRM practices
- Updated with latest Threat Information

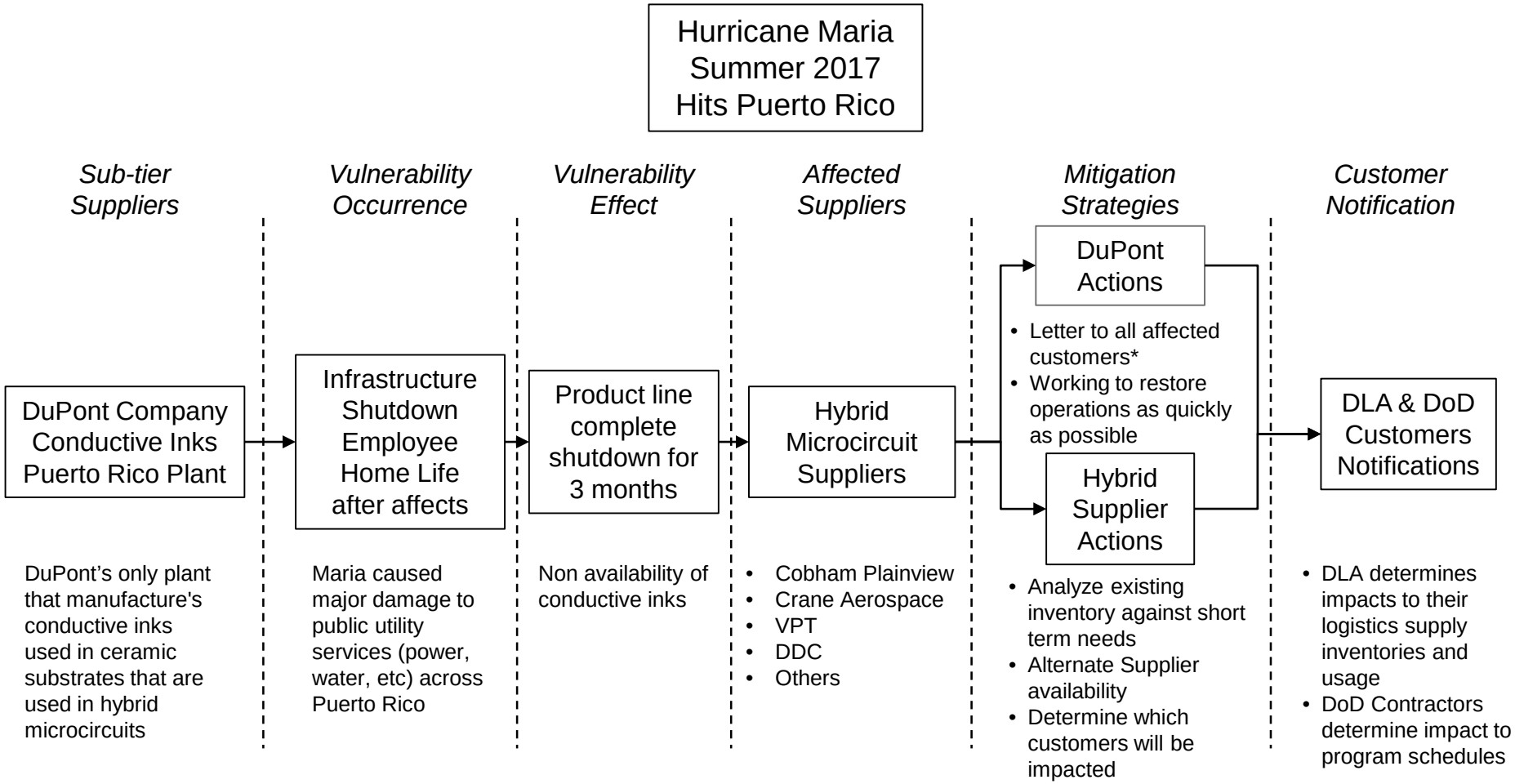
Class is available to any USG PO and cleared DoD Contractors

- ***Must have TS/SCI facility clearance***
- ***Contractors require GPO authorization***

- Been given to 13 different government program offices across the DoD, ODNI and NASA
- The following Contractors have received the briefing:
  - Boeing El Segundo
  - NGAS (x2)
  - NGES (BWI)
  - Ball (x3)
  - LMSSC (x2)
  - SEAKR
  - GD – AIS (Scottsdale)
  - Honeywell (Glendale & Clearwater)
  - Harris (Rochester & Palm Bay)
  - Harris (L3 S&NS)
  - Collins Aerospace (UTAS)

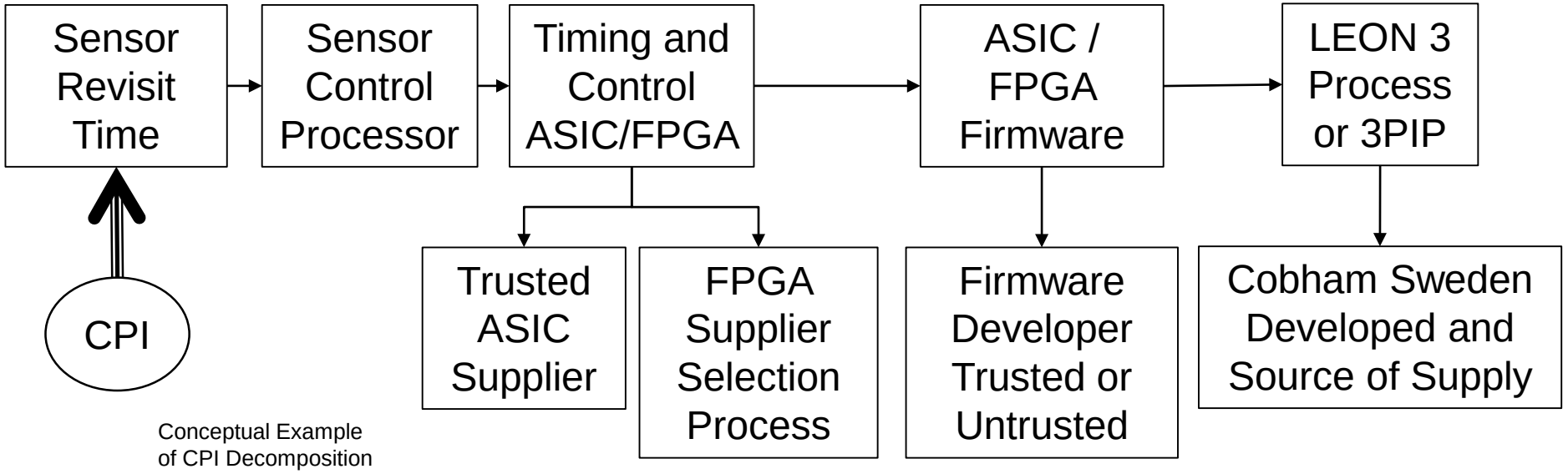
Back-up Charts

Why Knowing Your Supply Chain Is Important



* FORCE MAJEURE EVENT AT DUPONT ELECTRONIC MATERIALS PLANT IN PUERTO RICO, letter issued October 6, 2017

Functional Decomposition of CPI to Component Implementation



Conceptual Example of CPI Decomposition

- Systems Engineering is responsible for the functional decomposition and allocation of CPI into system functions
- Design engineering is responsible for implementing these functions into system hardware and software
- Mission Assurance and PM&P identify the PM&P and firmware and then start the Counter Intelligence Process

Foreign Supplier Assessment

Compliance to DoD Instruction 5200.39

- Foreign suppliers need to be vetted to determine if they are at risk for hostile foreign intrusion and exfiltration of restricted data
  - *Foreign suppliers are more susceptible to compromise*
    - Lack of technology export controls
    - Customer electronic access to their systems
- To vet a foreign suppler is the same process for vetting CPI component suppliers.
- Due to the time it can take for the CI community to complete an assessment, foreign supplier need to be identified as early in the program schedule as possible.