National Aeronautics and Space Administration

IT & Communications Supply Chain Risk Management (ITC SCRM)

NASA CIO

Kanitra Tyler
10/25/2018

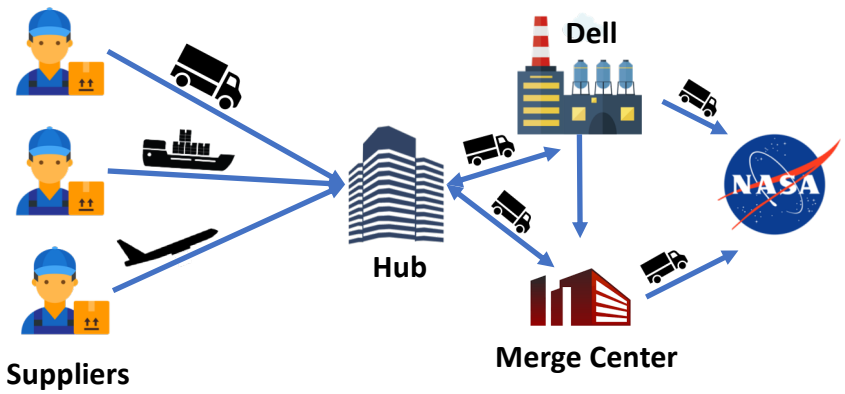
What is Supply Chain?

Have you ever wondered where your everyday household items come from?

From your phone to refrigerator, these products have gotten to you by efficient supply chains.

A supply chain is the process of getting a product from point A to point B.

In more specific terms, a supply chain is the inclusion of all individuals, resources, organizations, and technology used in the sale and delivery of a product.



What is Supply Chain?

<1% Corn Syrup

Soy Lecithin

Chocolate

Cocoa Butter

Lactose

Salt

Milk

Sugar

Cornstarch

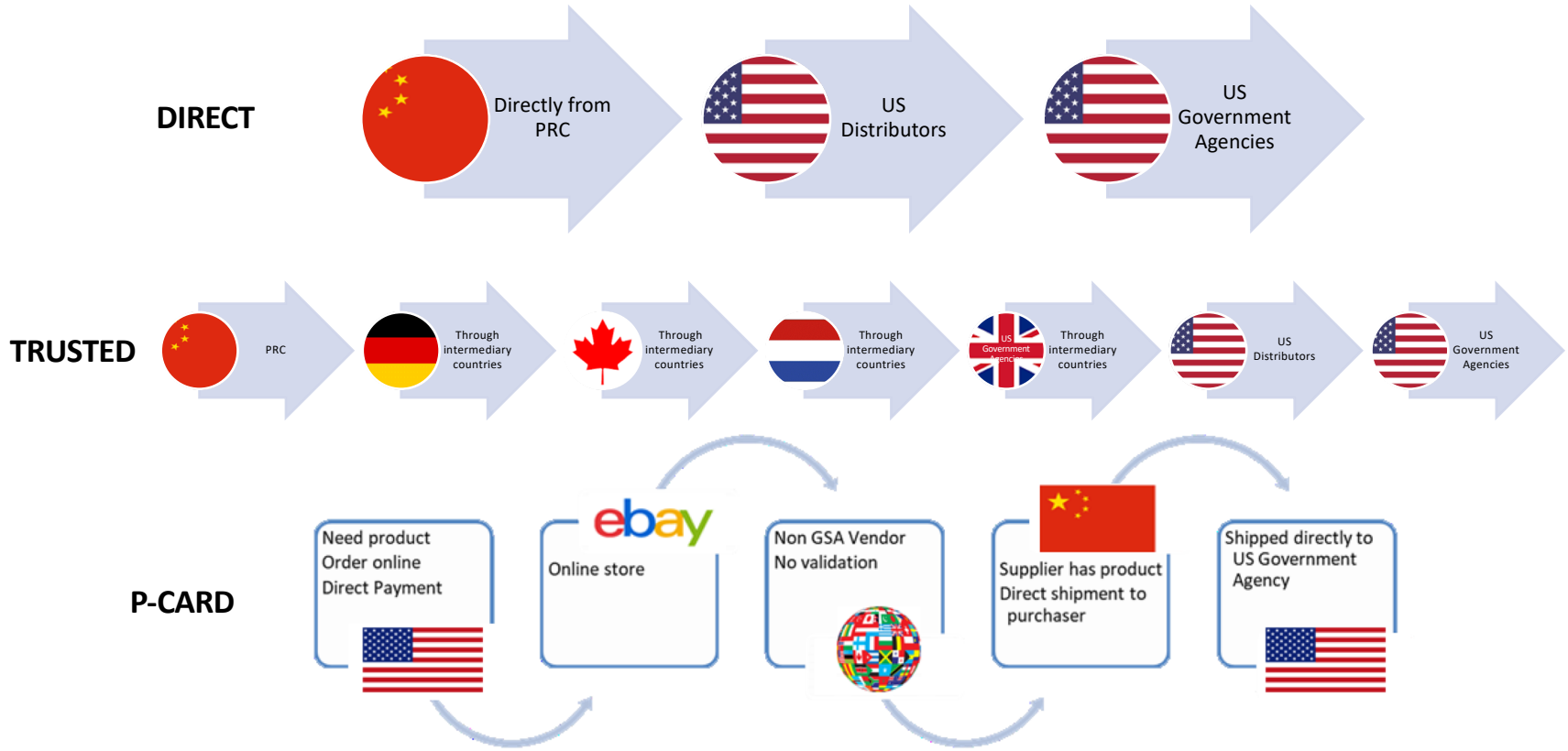
What is SC Risk Management?

A supply chain is the link between all facets of the successful delivery of a product.

- Supply Chain Risk Management Analysts play a key role in lowering the threats and vulnerabilities associated with the acquired information and communication technologies.

- SCRM allows system engineers to decrease the overall risk to government and businesses' systems and component sources.

Distribution Channels

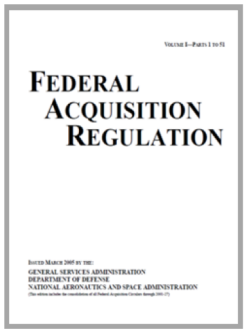


What are the Federal Drivers

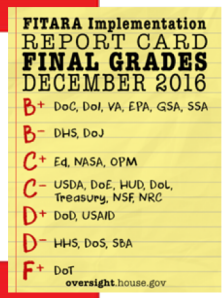
OMB A-130
Management of Federal Information Resources - 1985-2016

FISMA
Federal Information Security Modernization Act - 2014

John S. McCain National Defense Authorization Act 2019
Authorizes FY2019 appropriations and sets forth policies regarding the military activities of DoD



FAR Guidance:
Issued by the General Services Administration, the Dept. of Defense, and NASA



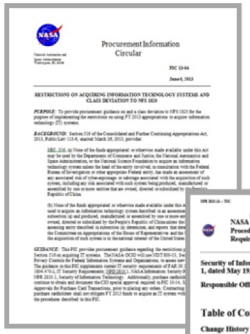
FITARA:
Enables enterprise-wide strategy for making smarter, business-enabling IT investments

NIST SP 800-37:
Guide for Applying the Risk Management Framework to Federal Information Systems

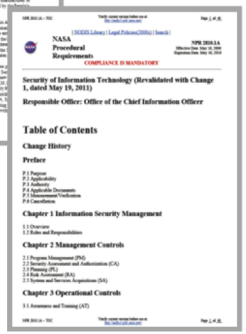
NIST SP 800-53:
Security and Privacy Controls for Federal Information Systems and Organizations

NIST 800-60:
Guide for Mapping Types of Information and Information Systems to Security Categories

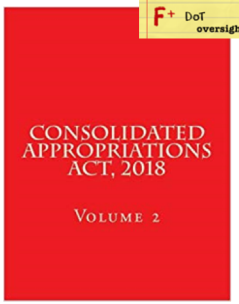
NIST SP 800-161:
Supply Chain Risk Management Practices for Federal Information Systems and Organizations



Procurement Class Deviation 15-03C:
(Sept. 11, 2018) Implements Consolidated Appropriations Acts



NPR 2810.1:
NASA Procedural Requirements: Security of Information Technology



Consolidated Appropriations Act, 2018, SEC. 514
Issued by Congress requiring Federal agencies to perform risk assessments for acquisition of Moderate- or High-impact systems

National Defense Authorization Act (NDAA) for Fiscal Year 2018

Section	
807	**Process for integrating SCRM into overall acquisition decision making**
1634	**Remove and permanently ban Kaspersky products and services**
1646	Prepare a briefing on cyber applications of blockchain technology
1659	Issue a policy establishing the prioritization of SCRM programs

John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019

Section	
881	**Permanent SCRM Authority**
889	**Prohibition of certain telecommunications & video surveillances or equipment.**
1613	Evaluation and enhanced security of supply chain for protected satellite communications programs and overhead persistent infrared systems
1644	**Assistance for small manufacturers in the supply chain and universities on matters relating to cybersecurity**
1657	Report on enhancement of software security for critical systems

NASA Scorecard

A
B
C
D
F

OGR Biannual Scorecard - May 2018

Agency	Nov '15 Grade	May '16 Grade	Dec '16 Grade	Jun '17 Grade	Nov '17 Grade	May '18 Grade	Agency CIO authority enhancement Incremental	Transparency and risk management Dashboard	Portfolio review PortfolioStat	Data center optimization Initiative DCOI	Software Licensing MEGABYTE	Modernizing Government Technology MGT	Cyber FISMA	CIO's boss = Sec/Dep Sec	CIO Status
NASA	F	F	C+	C+	C+	C+	F	F	A	B	A	C	F	Y	Permanent
Changes		▲ 0 ▬ 0 ▼ 0	▲ 12 ▬ 11 ▼ 1	▲ 4 ▬ 15 ▼ 5	▲ 3 ▬ 15 ▼ 6	▲ 5 ▬ 8 ▼ 11	All software pro	Tiers DOD alt source	Tiers JSONS	50-50 Bumps	Include	Include	Exclude	Y-N drop	

																		⇧ from 12 Y	⇧ from 18
A						▲	1	▬	1	▼		15	5	5	4	8			15 Y	20 permanent
B	2	▼	1	▲	8	▼	7	▼	4	▲	3	4	5	5	5		3		9 N	4 acting
C	5	▲	12	▼	10	▬	10	▲	14	▲	12	1	5	5	8	2	12	5		
D	14	▼	10	▼	5	▬	5	▼	3	▲	8		5	5	2		6	9		
F	3	▼	1	▬	1	▬	1	▲	2	▼	1	4	4	4	5	14	3	9		

Where we are & Where we want to go?

Current

- Process is Ad Hoc
- Process is Reactive
- Does not consistently coordinate with FBI
- Cybersecurity program remains ineffective
- Practices do not require IT & COMM Product Testing
- Excludes specific IT systems and flight HW
- Purchase of non-vetted IT and ICT assets

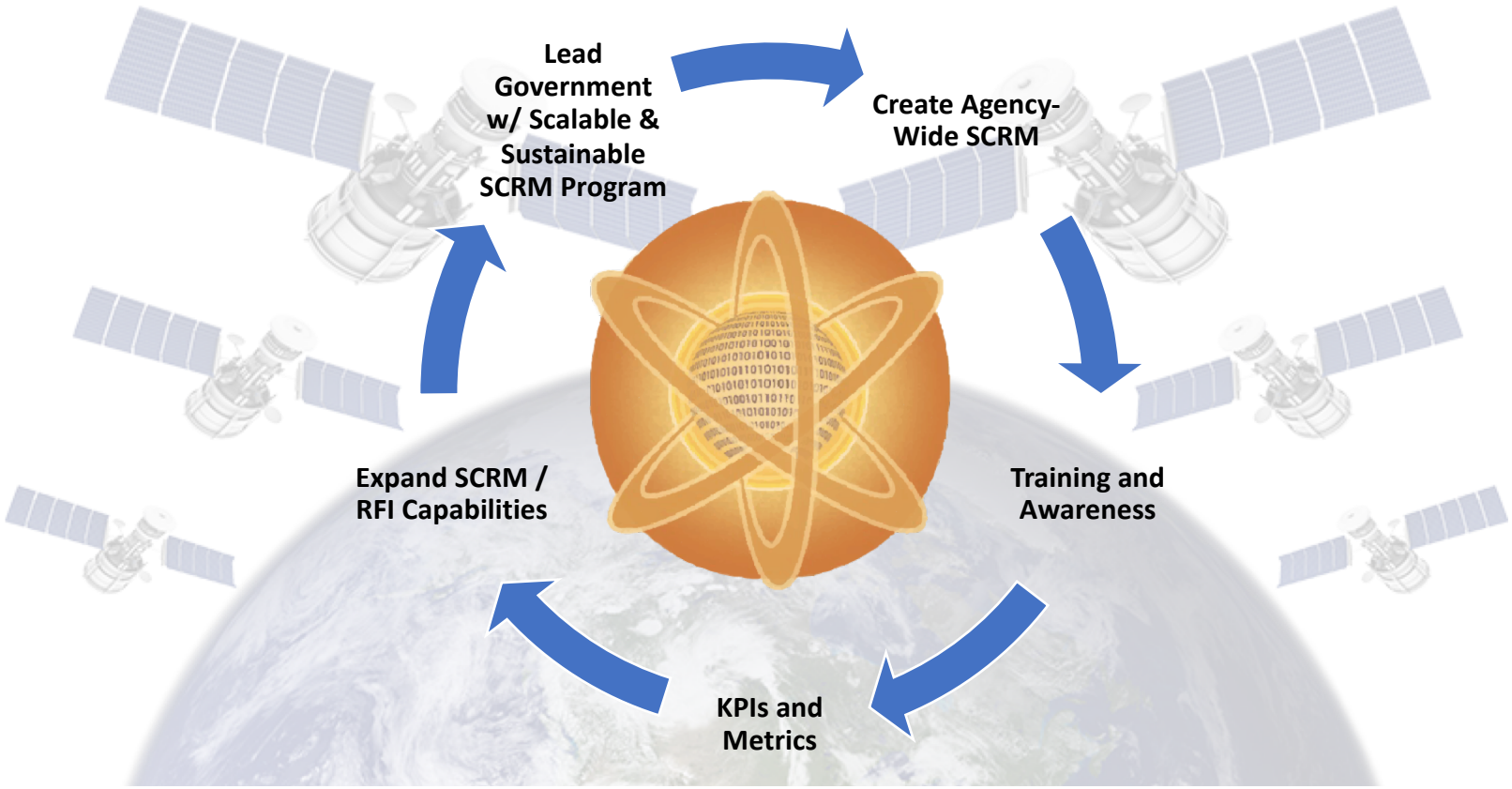
Future

- Proactive Process
- Alignment of IT solutions with mission & customer needs
- LINK CIO chain and programmatic chain for IT decision making
- Create comprehensive agency-wide SCRM capability
- Process to prioritize analysis of sub-tier visibility
- Identify, document & prioritize dependencies
- Continuous monitoring of suppliers
- Expand current SCRM / RFI capabilities

Challenges

- Inefficient implementation
- Inconsistent implementation
- Limited skillsets
- Limited Resources
- Procurement regulations, processes & integration

Scope & Expectations



Timeline

FY Q1 - IOC

- Centers SCRM inventory compilation
- Process, Procedure and CONOPS development
- Initial Supplier List Collection
- Engage cross Center SCRM reps
- Begin populating portal and sharing across Centers
- Implement Agency-wide KPI and Metrics capture and sharing
- Charter
- Risk Tolerance Questionnaire

FY Q2 - Q3

- Deliver FY19 Q1 KPIs and Metrics
- Continued Supplier Assessment and Continuous Monitoring Sharing
- Deliver FY19 Q2 KPIs & Metrics
- Scoping Agency-wide scaling of program
- Implement KPIs & Metrics Reporting Process for Congressional, OMB, and Agency Leadership

FY Q4 - FOC

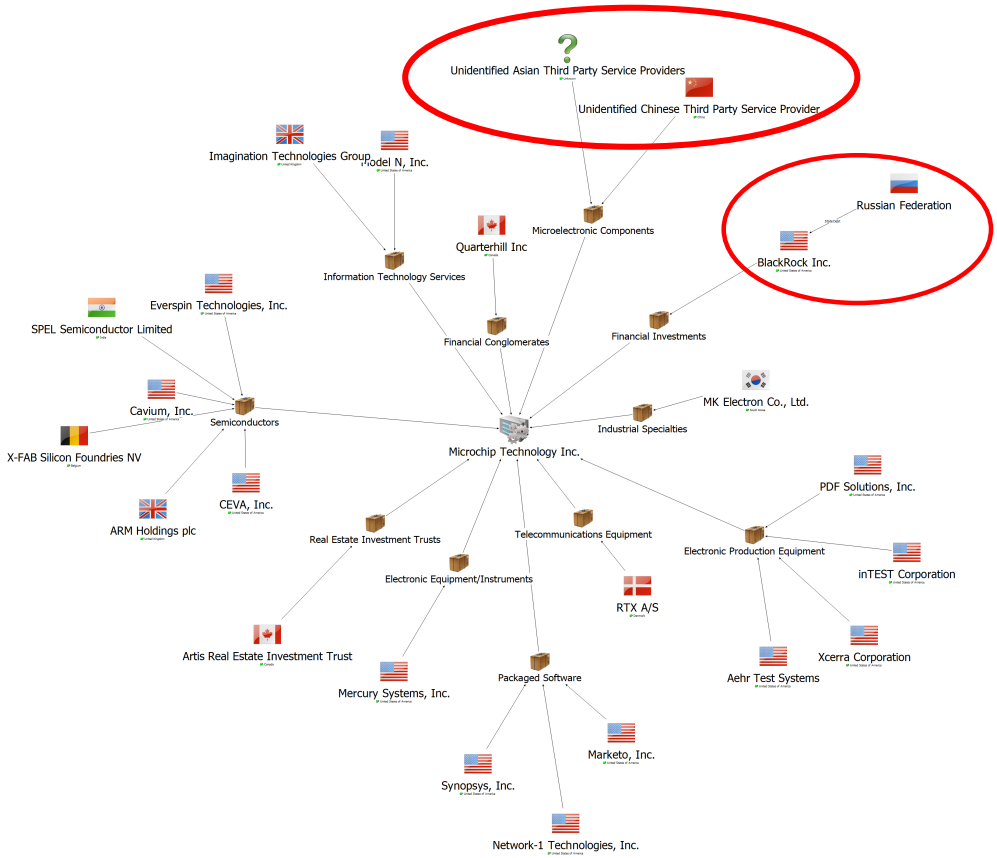
- Deliver FY19 Q3 KPIs and Metrics
- Engage external Agencies and Industry
- Re-prioritize current continuously monitored suppliers and prioritize FY20 Q1 suppliers

Autonomous Vehicles Hack

Microchip Assessment

- Microchip Technology – Chandler, Arizona
- Concerns
  - Quality Assurance
    - 15 Products Since 2014 Nonconforming or Counterfeit
  - Production and Manufacturing
    - Outsourced Product Testing and Assembly to Several Asian Countries
  - Business Alliances
    - Announced 2018 Collaboration with China Telecom – 100% Chinese Government Controlled
  - Revenue and Financial
    - Blackrock Incorporated owns a 6% share of Microchip – Russian Held Company

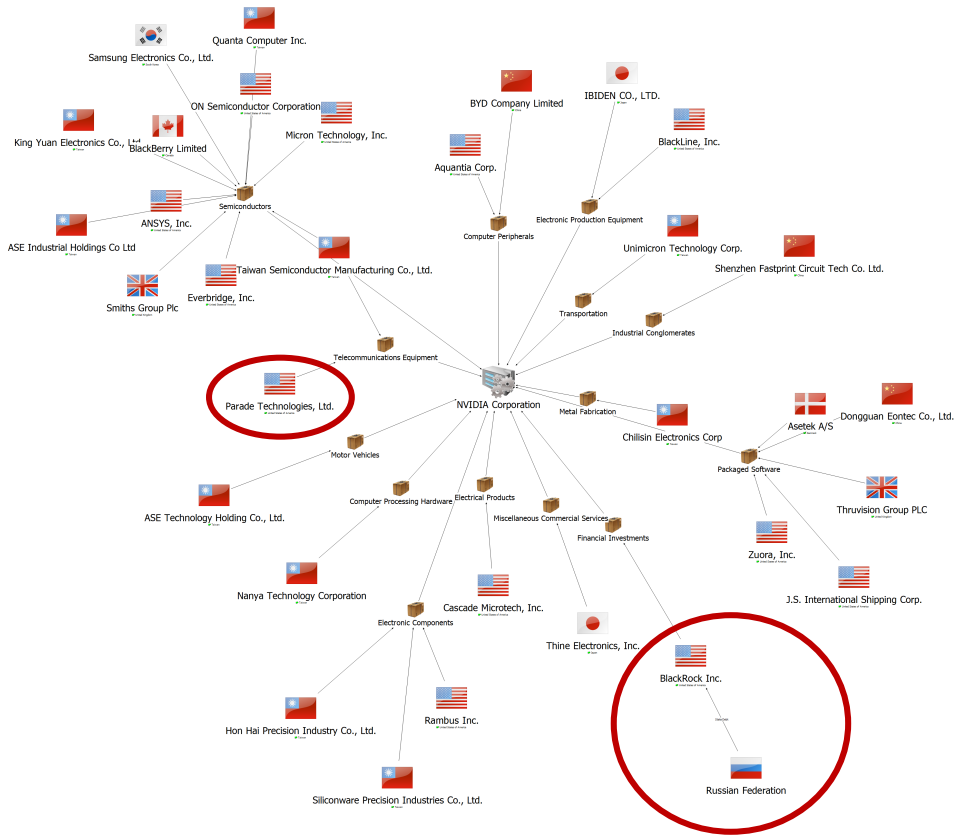
IT Microchip Ecosystem



NVIDIA Assessment

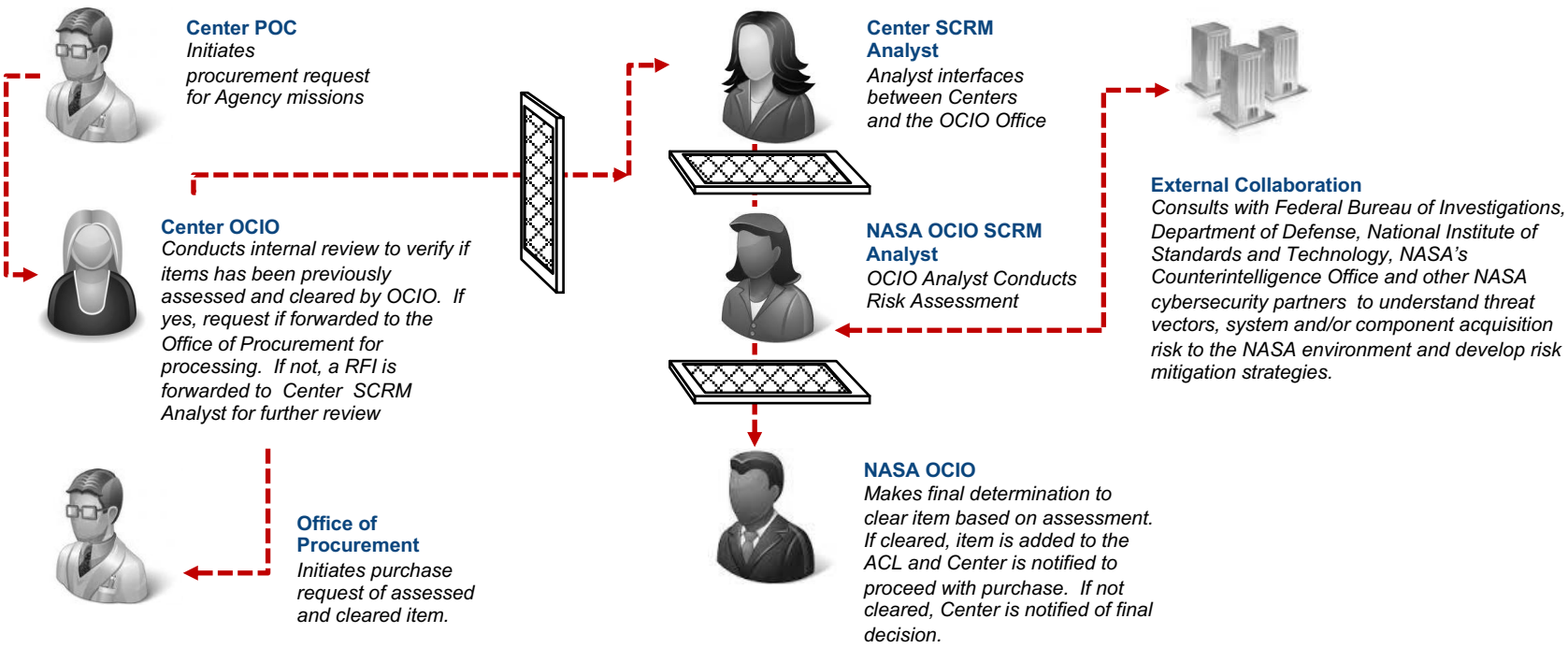
- NVIDIA Corporation– Santa Clara, California
- Concerns
  - Quality Assurance
    - Outsourced Quality Testing to Hong Kong, China and Taiwan
  - Production and Manufacturing
    - Fabless Manufacturing Strategy – Outsources Fabrication, Assembly and Testing
  - Regulatory and Legal
    - 2015 Class Action Lawsuit for False Claims with Graphics Card Performance
    - 2018 Patent Infringement Lawsuit Seeking Damages and Injunctions
    - Intellectual Property Theft Possible from Chinese Government Subpoenas
  - Revenue and Financial
    - Blackrock Incorporated owns a 6.21% share of NVIDIA – Russian Held Company

IT NVIDIA Ecosystem

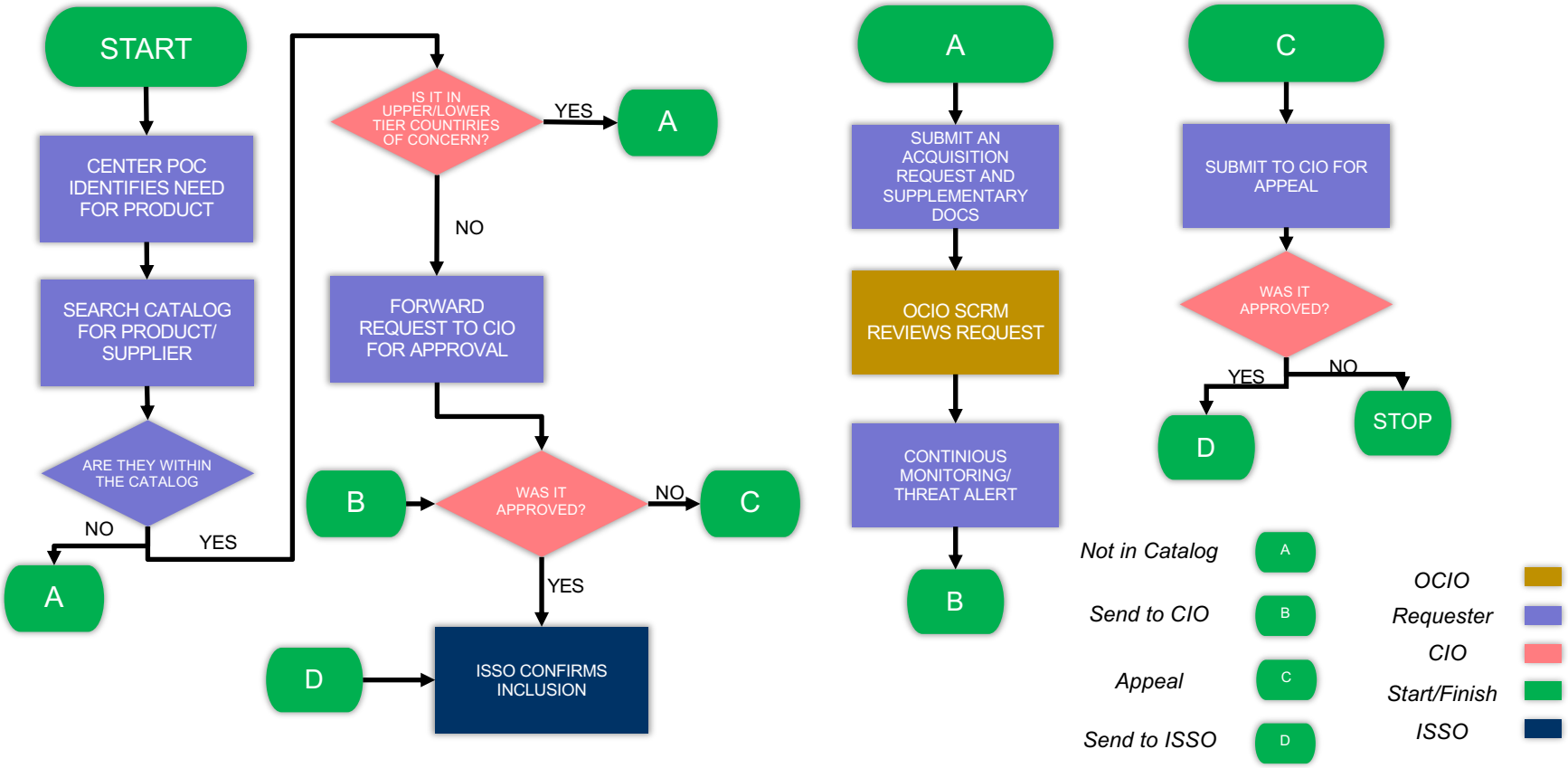


Current Process

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

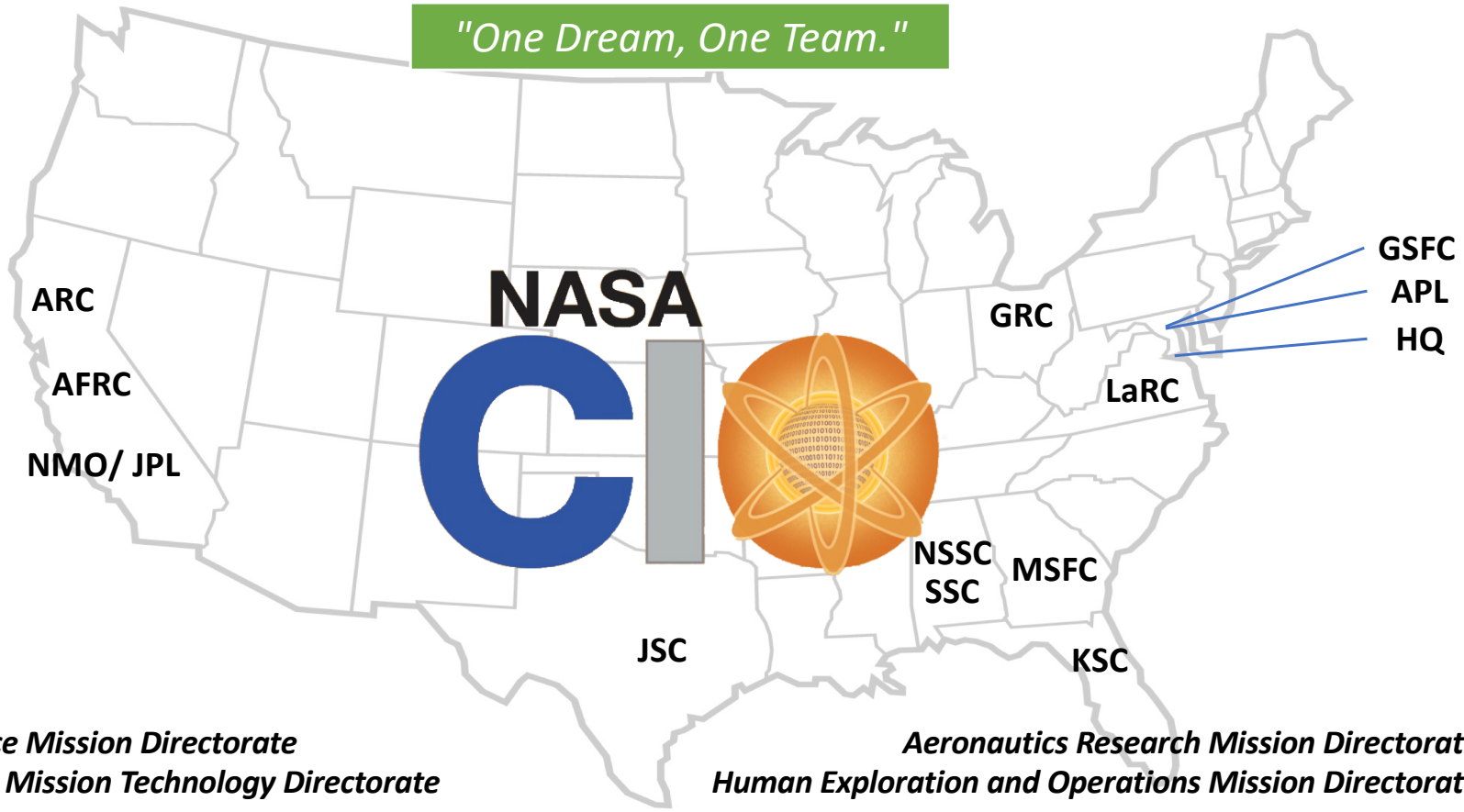


Future Process



Who OWNS the risk?

"One Dream, One Team."



Science Mission Directorate
Space Mission Technology Directorate

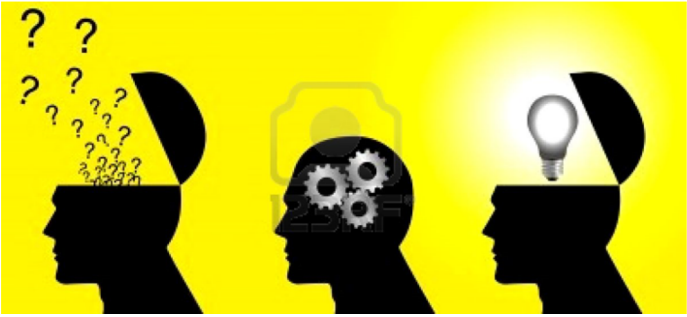
Aeronautics Research Mission Directorate
Human Exploration and Operations Mission Directorate

How to get help?

Agency ITC SCRM Service Manager, Kanitra Tyler, Kanitra.D.Tyler@nasa.gov, 301-286-6173

Center	POC	Center	POC
ARC	Kay Twitchell	KSC	Paul Kostka
AFRC	Shannon Walsh	LaRC	Robert Quinn
GRC	Vinh Le	LaRC	Kenny Nichols
GRC	Jocelyn Mendez	LaRC	Mike Knight
GRC	John Ferguson	MSFC	Leslie Barbee
GSFC	Donnell Lassiter	NSSC	Darryl Smith
GSFC	Dawn McGowan	SSC	David Walters
HQ	Darren Gunlock	SSC	Teenia Perry
HQ	Bradley Rowbottom	SSC	Bonita Oliver
JPL	James Rinaldi	SSC	Scot Gressaffa
JSC - primary	Ann Whitener		
JSC	Michale Bauer		
JSC	Kelly Reid		a/o 09.11.18

What Do We Need From you?



Questions & Discussion

Thank you!