



NASA EXPLORES

**Supply Chain Security and Mission Assurance:
*Legislation Drivers, NASA Policies, and Best Practices***

Jonny Pellish
NASA Electronic Parts Manager
jonathan.pellish@nasa.gov



Outline

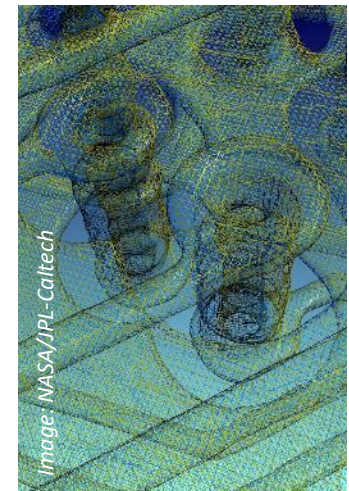
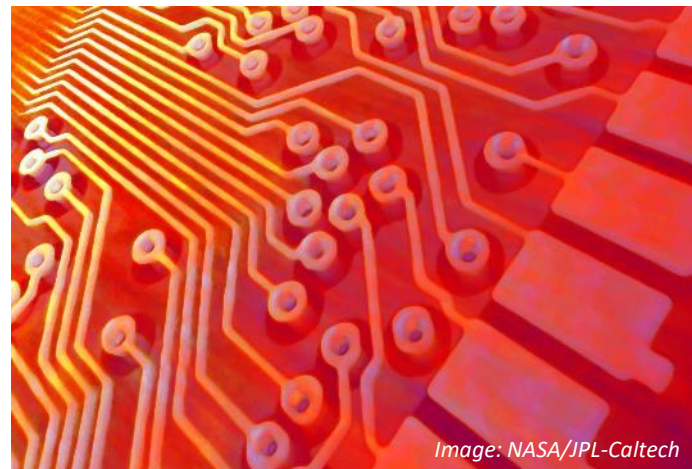
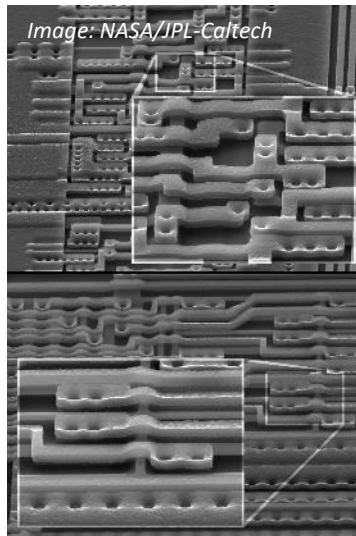
- Our current reality (...admittedly a snapshot from one perspective...)
- Supply chain risk management (SCRM) and using the term “supply chain security”
- Statutory, regulatory, policy, and process landscape
- Becoming proactive and harmonizing stakeholder approaches

Important to understand that SCRM in this presentation’s context is tied to information and communications technology, which in turn leads us to microelectronics (what we call electrical, electronic, electromechanical, and electro-optical (EEEE) parts, components, assemblies)

What is our focus for today?

Integrating with Agency processes that identify, assess, and mitigate the risks associated with the global and distributed nature of product and service supply chains (*especially for cyber / malicious threats*)

All about microelectronics, at least for this discussion – will fall under the umbrella of information and communications technology (ICT)



What is our current reality?

Significant focus on ICT by legislators, policymakers, and technical professionals



<https://news.fnal.gov/2020/10/solid-state-technology-for-big-data-in-particle-physics/>

<https://inl.gov/trending-topic/5g-wireless-technology/>

Laws and policies are targeting these systems



Image: NASA

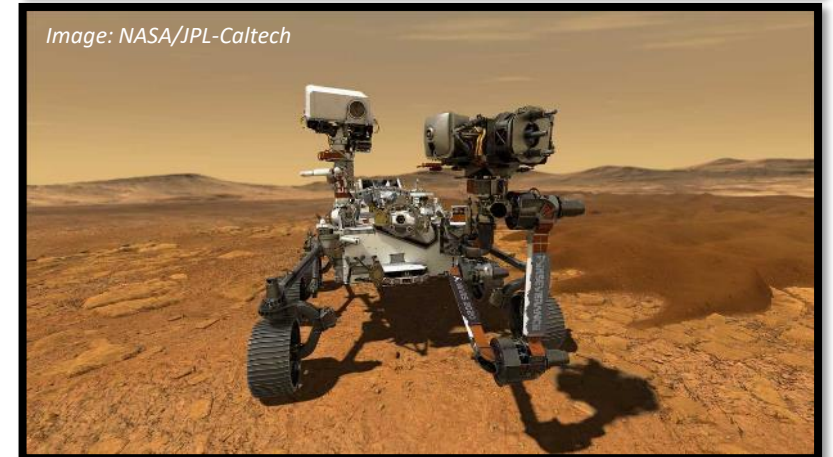
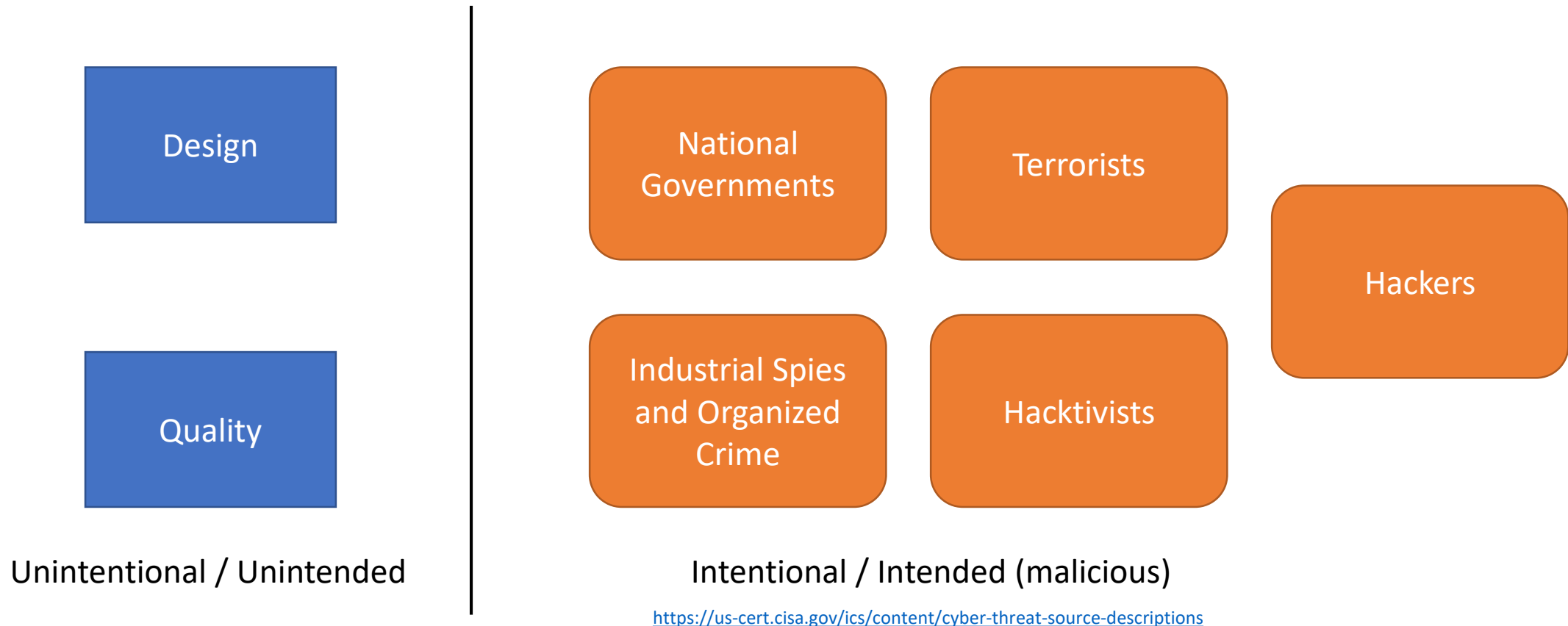


Image: NASA/JPL-Caltech

How do we adapt for these systems?

Threat space for all of us has evolved

Civil space is evolving its risk posture – like what other organizations have been doing
Maintain same processes / practices as well as add new ones





Supply Chain Risk Management & Supply Chain Security

What is (ICT) supply chain risk management?

- ICT SCRM is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of Information Technology (IT)/Operational Technology (OT) product and service supply chains
 - Will not be covering OT in this presentation
- SCRM is an overloaded term in many organizations (NASA is no exception) – means different things to different stakeholders
 - Split between institutional SCRM and mission-focused SCRM

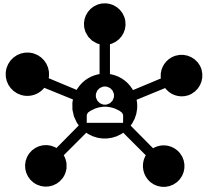
From a NASA perspective, we are attempting to normalize the term “supply chain security” when talking about cyber or other types of malicious threats in the context of mission-specific product and service supply chains

Differentiate from institutional contexts, though many / most of the stakeholders are the same

What is (ICT) supply chain risk management?

- ICT SCRM covers the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction) as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an IT/OT product or service at any stage
- NASA ICT SCRM generally focused around 3 “P’s”

Provenance



Transparent, traceable, and tamper-proof supply chain data.

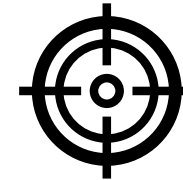
Each link in the supply chain being able to trust the link before and after it.

Pedigree



Tracking of manufactured products through distribution channels prevents counterfeiting and ensures safety and security of products.

Position



Innovation and efficiency in contracting management with provider optimization and redundancy.

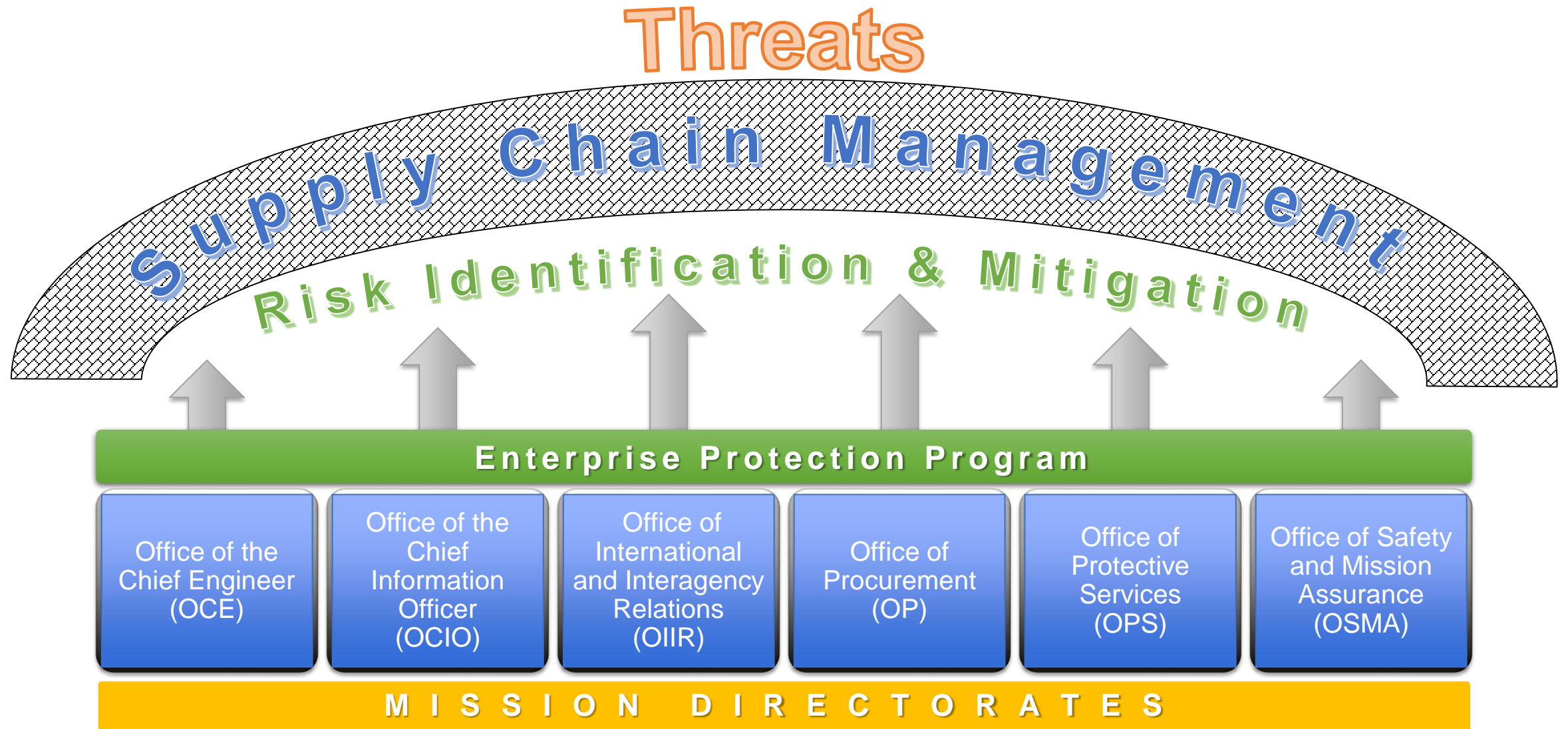


Supply Chain Security

- From NPR 1058.1 §1.1 – the NASA Enterprise Protection Program:
 - *Current trends* in the proliferation of technology and technical information, accessibility to space, globalization of space programs and industries, and foreign knowledge about U.S. space and aeronautical systems *increase the threat environment to NASA* flight systems, ground systems, and supporting infrastructure.
 - This heightened threat environment *increases the possibility that* NASA flight systems, ground systems, and supporting *infrastructure could be subject to a disrupted, degraded, or denied environment, or a direct attack*, through a variety of means and methodologies.
- Monitoring and mitigating these dynamic threats for flight hardware (and software) requires the implementation of SCRM

The Enterprise Protection Program has established several working groups to tackle challenges, like supply chain security, as part of its Zero-Based Review process

Many NASA Stakeholders Required for Mission Success



Supply Chain Management Roles

OCE

- Industrial base policy & critical at-risk industrial technologies list
- Mission Resilience and Protection Program

OCIO

- ICT SCRM service owner

OIIR

- Department of Defense and Intelligence Community liaisons
- Export Control

OP

- Federal Acquisition Regulation (FAR)
- NASA FAR Supplement (NFS) / Procurement Class Deviations (PCDs)

OPS

- Counterintelligence
- Intelligence

OSMA

- Quality Assurance & SCRM



Laws, Regulations, Policies, and Processes

What drives ICT SCRM for us?

Federal Drivers

Institutional Drivers

Laws

Regulations
(Federal Acquisition Regulation (FAR))

Executive Orders

NASA Policy Directives (NPDs)

NASA Procedural Requirements (NPRs)

Procurement Policies and Requirements

Cadence of change is accelerating rapidly

Mandatory vs. Discretionary

Recent Federal Laws (not exhaustive)

- John S. McCain National Defense Authorization Act for Fiscal Year 2019 ([Pub. L. 115-232](#))
 - Sec. 889: Prohibition on certain telecommunications and video surveillance services or equipment
- Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE) Technology Act ([Pub. L. 115-390](#))
 - Title II: Federal Acquisition Supply Chain Security Act of 2018
 - Created the Federal Acquisition Security Council (FASC)
- Consolidated Appropriations Act, 2021 ([Pub. L. 116-260](#))
 - Sections 208 & 514
 - Consolidated Appropriations Act, 2020 ([Pub. L. 116-93](#)) also had provisions
- Earlier laws (<2018) generally directed agencies to establish policies / procedures (except SECURE Technology Act) – while recent laws have been more prescriptive in terms of what agencies can / cannot procure

Recent Regulations (not exhaustive)

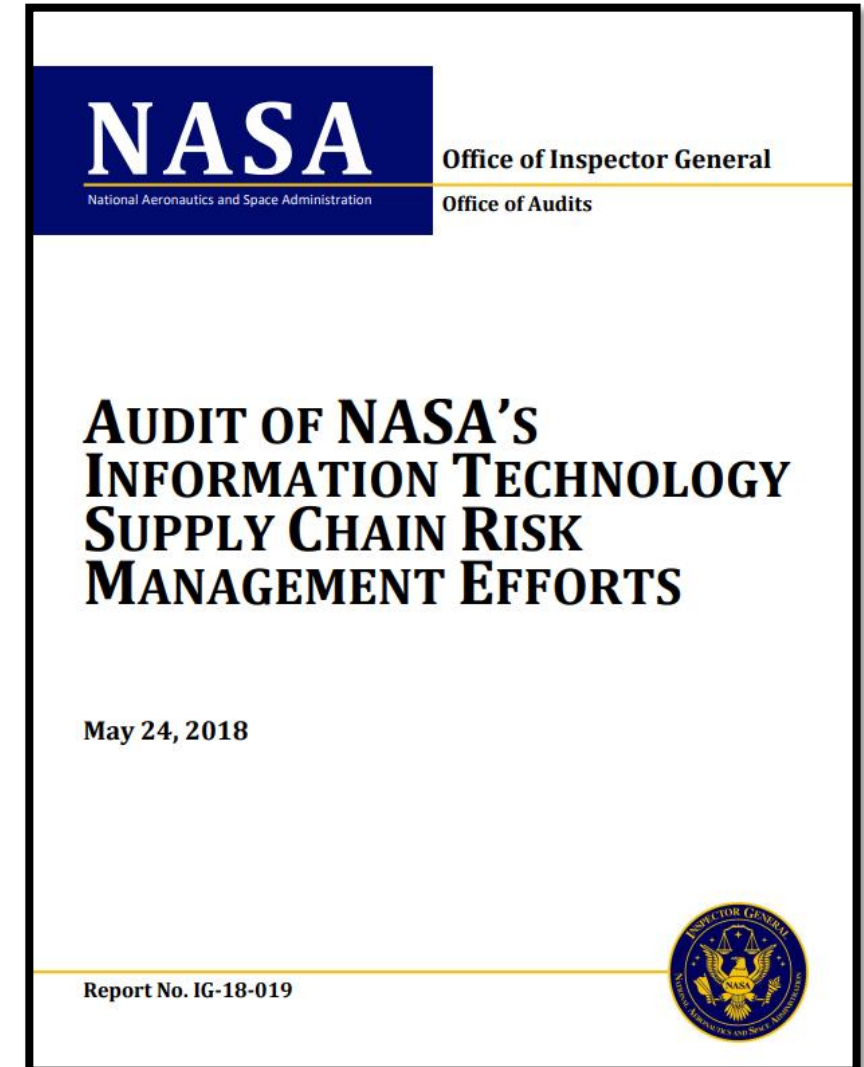
- Federal Acquisition Circular [2019-05](#) / [2020-03](#)
 - Implementation of Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019
- Federal Acquisition Circular [2020-08](#) / [2020-09](#)
 - Implementation Section 889(a)(1)(B) of Title VII of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019
- Recommended FAR Case 2021-XXX (Reporting Cyber Incident and Threat Information for Information and Communications Technology)
- FAR [52.204-23](#) through [52.204-26](#)
 - Updated / amended based on above Federal Acquisition Circulars
- NASA Procurement Class Deviation [\(PCD\) 15-03D](#)
 - CLASS DEVIATION TO NFS PARTS 1839 AND 1852, RESTRICTIONS ON ACQUIRING MODERATE OR HIGH-IMPACT INFORMATION TECHNOLOGY SYSTEMS
 - Primary NASA procurement implementation mechanism for ICT SCRM until all FAR rules are finalized

Recent Executive Actions (not exhaustive)

- OMB revised [Circular A-130](#) in 2016 requiring Federal agencies to develop supply chain risk management plans as described in NIST [Special Publication \(SP\) 800-161](#) (Supply Chain Risk Management Practices for Federal Information Systems and Organizations); NIST SP 800-161 being revised now
- [Executive Order 13806](#) (July 21, 2017): Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States
- [Executive Order 13873](#) (May 15, 2019): Securing the Information and Communications Technology and Services Supply Chain
- [Executive Order 14017](#) (February 24, 2021): America's Supply Chains
- [Executive Order 14028](#) (May 12, 2021): Improving the Nation's Cybersecurity
- [Executive Order 14034](#) (June 9, 2021): Protecting Americans' Sensitive Data From Foreign Adversaries
 - Elaboration on E.O. 13873

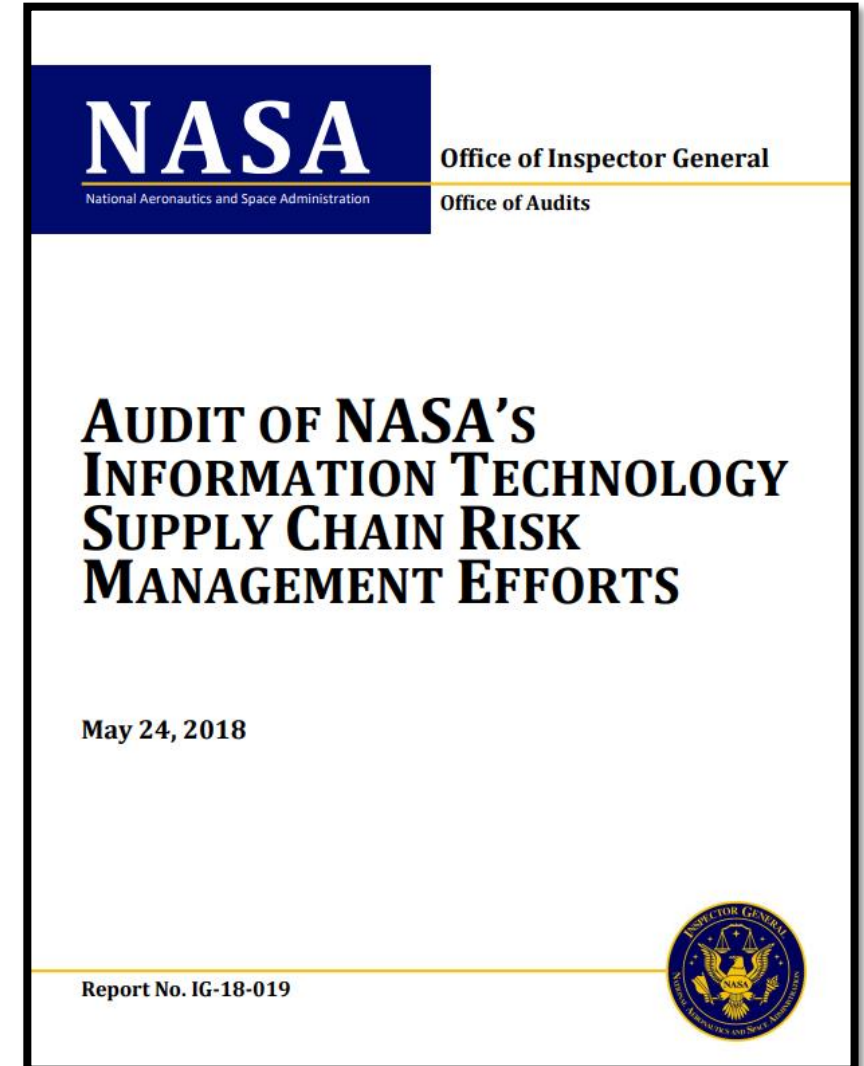
Report No. [IG-18-019](#) (NASA OIG)

- Provides excellent history of legislation, regulation, and policy to point of publication
- Recommendation #3: Revise the NASA Procurement Class Deviation to remove language that exempts IT systems from the Agency's supply chain risk management review process.
 - "...the Deviation further defined moderate or high-impact IT systems by categorizing items such as embedded IT (used as an integral part of another product), flight hardware (including equipment operated on the International Space Station), and prototypes used to test, troubleshoot, and refine air and spacecraft hardware and software that does not fall within the definition of an IT system."
 - "Our review of NIST definitions of "Information System" and "Information Technology" leads us to conclude that it was not the intent of the legislation to exclude such critical components as imbedded IT, where such technology is integral to the system or component's operation."



Report No. [IG-18-019](#) (NASA OIG)

- When NASA PCD 15-03 was revised as a result of accepting the audit report's findings and recommendations, it had the effect of putting engineering and flight EEEE parts in scope for all procurement restrictions and all ICT SCRM processes
- What do we do now?
 - For EEEE parts, components, and assemblies, figure out what's in / out of scope
 - Integrate existing identification, design, and acquisition processes with ICT SCRM processes

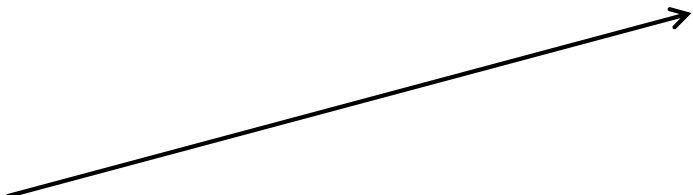




Reactive to Proactive – the path ahead

Define a “Covered Article”

- For our purposes, we rely on the definition of “covered articles” provided in the SECURE Technology Act (Pub. L. 115-390)
 - Covered article is defined as:
 - Information technology, as defined in 40 U.S.C. 11101, including cloud computing services of all types
 - [...omitted two additional definitions for brevity...]
 - Hardware, systems, devices, software, or services that include embedded or incidental information technology



“Embedded” and “Incidental” widen the scope for microelectronics / EEEE parts and components because it means that the inherent capability is what’s important – not necessarily the end use (e.g., if a part can perform function X-Y-Z, but you’re only using X, you still need to consider the scope and effect of X-Y-Z).

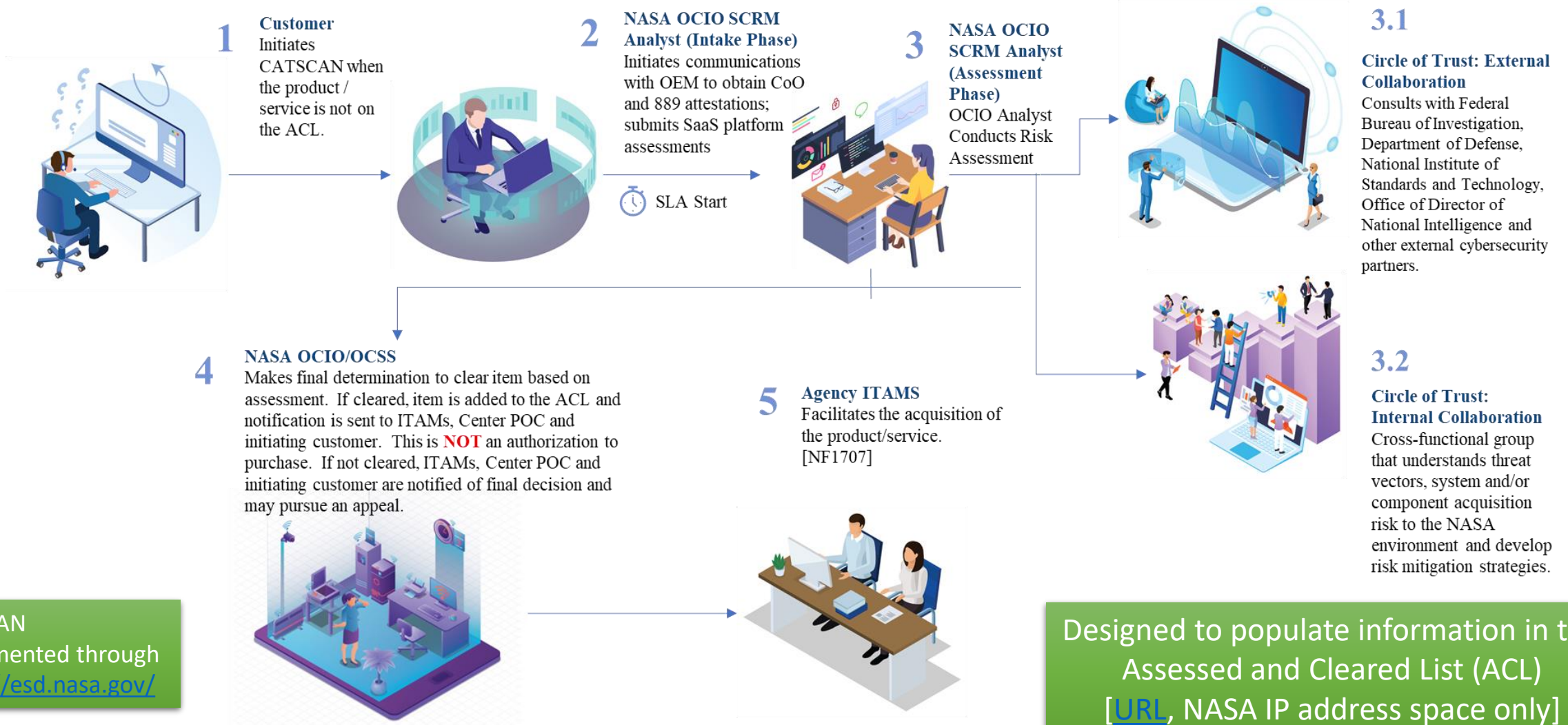
Define a “Covered Article”

- 40 U.S.C. 11101 (6) Information Technology
 - (A) with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use—
 - of that equipment; or
 - of that equipment to a significant extent in the performance of a service or the furnishing of a product;
 - Omitted (B) and (C) for brevity

Electronic Parts Management Approach to ICT SCRM

- Prior to January 2021, engineering and flight hardware (i.e., electronic parts and components) was submitted to ICT SCRM processes in an ad hoc fashion
 - Some proactive attempts were made, but most action was based on articles being flagged during the procurement process or in post-procurement audits
 - Variation from Center to Center, different views of what's in-scope / out-of-scope, etc.
- Since January 2021, GSFC and JPL have been working together on a joint process, based on groundwork laid by JPL, that attempts to triage compliance with ICT SCRM requirements
 - Current efforts will continue through JPL's contract compliance date for ICT SCRM
 - Then planning to roll out a process to all Centers with leadership / guidance from GSFC and JPL as the designated capability leaders for electronic parts management – *there will be growing pains and evolutions...*

Covered Article and Technology Supply Chain Assessment Needed (CATSCAN) Process [NASA ICT SCRUM Service]



CATSCAN implemented through <https://esd.nasa.gov/>

<https://nasa.sharepoint.com/sites/ictscrm>

Designed to populate information in the Assessed and Cleared List (ACL) [URL, NASA IP address space only]

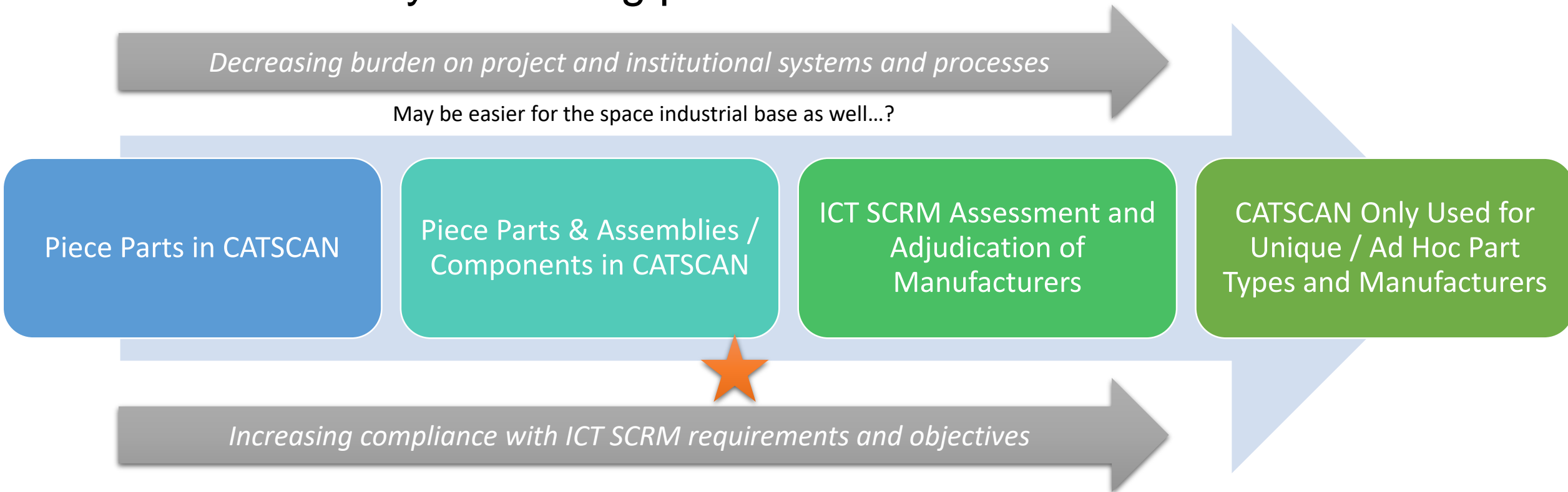
ICT SCRM Application to EEEE Parts Hardware

Category	Sub-Category
Memories (volatile)	DRAM/SDRAM/etc.
Memories (non-volatile)	EEPROM/NAND/NOR/etc.
Microcircuits	Analog-to-Digital (ADC) & Digital-to-Analog (DAC) Converters
Microcircuits	FPGA
Microcircuits	Processor/controller
Microcircuits	Mux/Demux
Microcircuits	Driver/Receiver/Transmitter
Sensors	Image Sensors
Systems-on-a-Chip (SOC)	All
Application-Specific Integrated Circuits (ASIC), Application-Specific Standard Products (ASSP)	All
Fully-assembled boards containing any of the above items	All

- This is the “Piece Part Filter” (PPF) used before any procurements as a screening tool for ICT SCRM services
- Purely mechanical parts are not applicable, including connectors, wire, etc.
- Passives and discrete semiconductors are not applicable, including capacitors, inductors, resistors, magnetics, diodes, MOSFETs, etc.
- Gray areas: hybrids, fully-assembled boards / standard products, hardware delivered through sub-contracts

Moving from Reactive to Proactive

- As discussed, using the CATSCAN process through ESD is eventually meant to be the exception rather than the rule – still using it now
- Paths to efficiency and being proactive




Next Steps

- Continue focusing on prioritized manufacturers and products
 - Based on “Piece Part Filter”
- Develop priorities for off-the-shelf assemblies / standard products
 - Things like global positioning system receivers, single-board computers, star trackers, etc.
- Migrate away from bottoms-up approach and move to top-down approach
 - Assess and clear at the manufacturer-level to populate the ACL with blocks of items instead of one at a time
- Refine processes for supporting out-of-house hardware acquisition
 - Primes and sub-contractors are bound by the same rules if they are using NASA appropriated dollars

Collective effort that requires increased cooperation and collaboration that can be maintained

Where can you look for more information?

- [FAR | Acquisition.GOV](#) / [NFS | Acquisition.GOV](#) / [NASA PCDs](#)
- Cybersecurity and Infrastructure Security Agency
 - <https://www.cisa.gov/supply-chain>
- NIST Computer Security Resource Center
 - <https://csrc.nist.gov/>
- NASA ICT SCRM Homepage (ICT SCRM Handbook, ACL, etc.)
 - <https://nasa.sharepoint.com/sites/ictscrm/>
- [Congress.gov](#)
- [Federal Register](#)
- [NODIS Library \(nasa.gov\)](#)
 - See NPR 1058.1, NPD 2810.1 and NPR 2810.1 in particular



*Thank you for your attention!
Questions welcome*

Acronyms

Abbreviation	Definition
ACL	Assessed and Cleared List
ADC	Analog to Digital Converter
ASIC	Application-Specific Integrated Circuit
ASSP	Application-Specific Standard Product
CATSCAN	Covered Article and Technology Supply Chain Assessment Needed
CoO	Country of Origin
DAC	Digital to Analog Converter
DRAM	Dynamic Random Access Memory
E.O.	Executive Order
EEEE	Electrical, Electronic, Electromechanical, and Electro-Optical
EEPROM	electrically Erasable Programmable Read-Only Memory
ESD	Enterprise Service Desk
FAR	Federal Acquisition Regulation
FASC	Federal Acquisition Security Council
FPGA	Field Programmable Gate Array
FY	Fiscal Year
GSFC	Goddard Space Flight Center
ICT	Information and Communications Technology
IP	Internet Protocol
IT	Information Technology
JPL	Jet Propulsion Laboratory
MOSFET	Metal Oxide Semiconductor Field Effect Transistor
NASA	National Aeronautics and Space Administration
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology

Abbreviation	Definition
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
OCE	Office of the Chief Engineer
OCIO	Office of the Chief Information Officer
OCSS	Office of Cybersecurity Services
OEM	Original Equipment Manufacturer
OIG	Office of Inspector General
OIIR	Office of International and Interagency Relations
OP	Office of Procurement
OPS	Office of Protective Services
OSMA	Office of Safety and Mission Assurance
OT	Operational Technology
PCD	Procurement Class Deviation
POC	Point of Contact
PPF	Piece Part Filter
QLF	Quality Leadership Forum
SaaS	Software as a System
SCRM	Supply Chain Risk Management
SDRAM	Synchronous Dynamic Random Access Memory
SECURE	Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure
SLA	Service Level Agreement
SOC	System on a Chip
SP	Special Publication
U.S.	United States
URL	Uniform Resource Locator