National Aeronautics and Space Administration

NASA's Proactive Supplier Engagement Process (PSEP)
Shared Services Forum

Kanitra Tyler, ICT SCRM Service Owner
Stefanie Manns, Task Lead

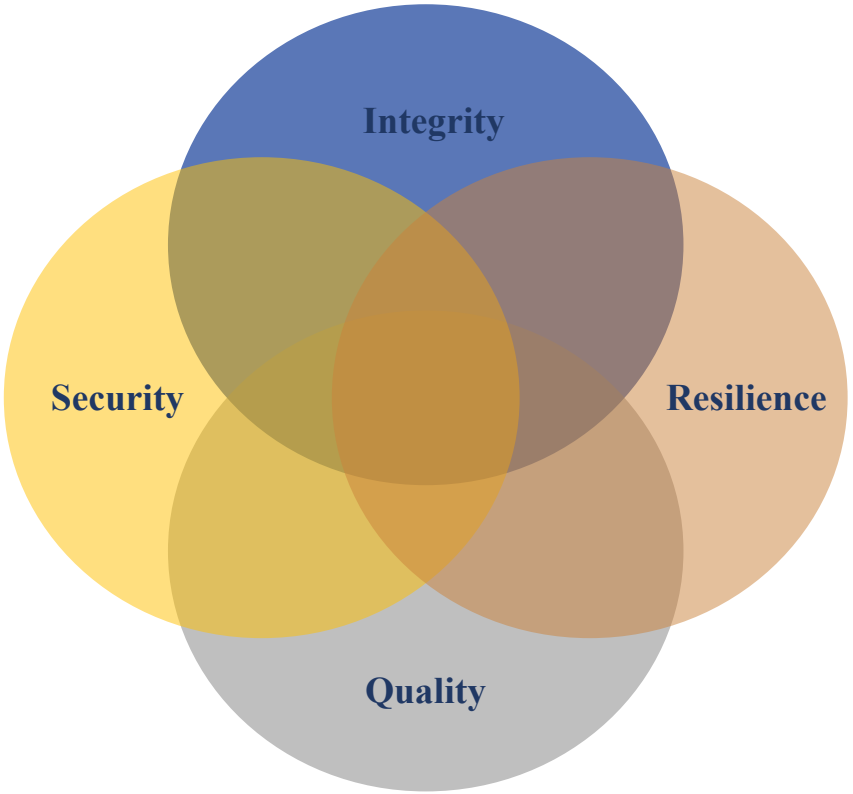
February 10, 2022

Agenda

- Bottom Line Up Front
- NASA OCIO Area of Responsibility
- NASA's Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Journey
- ICT SCRM Current & Future State
- Proactive Supplier Engagement Process (PSEP)
- Key PSEP Objectives
- NASA's ICT SCRM Toolkit
- NASA's Circle of Trust & Partnerships
- Q&A

Bottom Line Up Front

SCRM Takes a Village



Reactive State

PSEP

Proactive State

NASA OCIO Area of Responsibility

The term 'covered article' means—

(A) information technology, as defined in section 11101 of title 40, including cloud computing services of all types;

(B) telecommunications equipment or telecommunications service, as those terms are defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

(C) the processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program; or

(D) hardware, systems, devices, software, or services that include embedded or incidental information technology.

"Substantial or essential component" means any component necessary for the proper function or performance of a piece of equipment, system, or service

NASA's ICT SCRM JOURNEY

NASA ICT SCRM

2013

H.R. 933 (113th): Consolidated and Further Continuing Appropriations Act, **2013, Sec. 516.**

2014

H.R.3547 - Consolidated Appropriations Act, **2014, Sec. 515.**

2016

H.R.2029 - Consolidated Appropriations Act, **2016, Sec. 516.**

2017

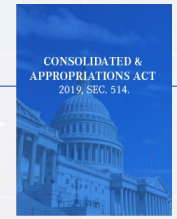
H.R.244 - Consolidated Appropriations Act, **2017, Sec. 515.**

2018

H.R.1625 - Consolidated Appropriations Act, **2018, Sec. 514.**

2019

H.R.648 - Consolidated and Appropriations Act, **2019, Sec. 514.**



2020 & 2021

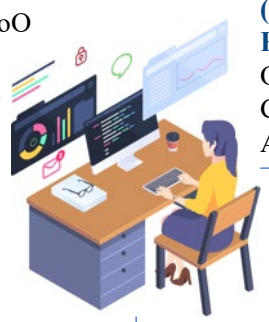
H.R.1158 & H.R.133 - Consolidated Appropriations Act, **2020 & 2021, Sec. 208 & Sec. 514.**

SCRM Current State: Covered Article and Technology Supply Chain Assessment Needed (CATSCAN) Process

1 **Customer**
Initiates CATSCAN when the product / service is not on the ACL.

2 **NASA OCIO SCRM Analyst (Intake Phase)**
Initiates communications with OEM to obtain CoO and 889 attestations; submits SaaS platform assessments

SLA Start



3 **NASA OCIO SCRM Analyst (Assessment Phase)**
OCIO Analyst Conducts Risk Assessment

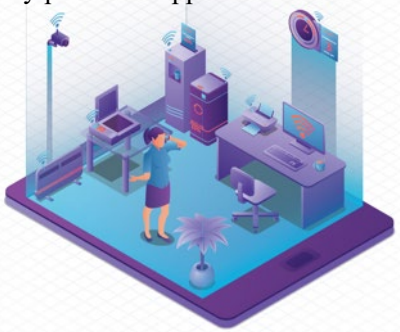
3.1

Circle of Trust: External Collaboration
Consults with Federal Bureau of Investigation, Department of Defense, National Institute of Standards and Technology, Office of Director of National Intelligence and other external cybersecurity partners.

3.2

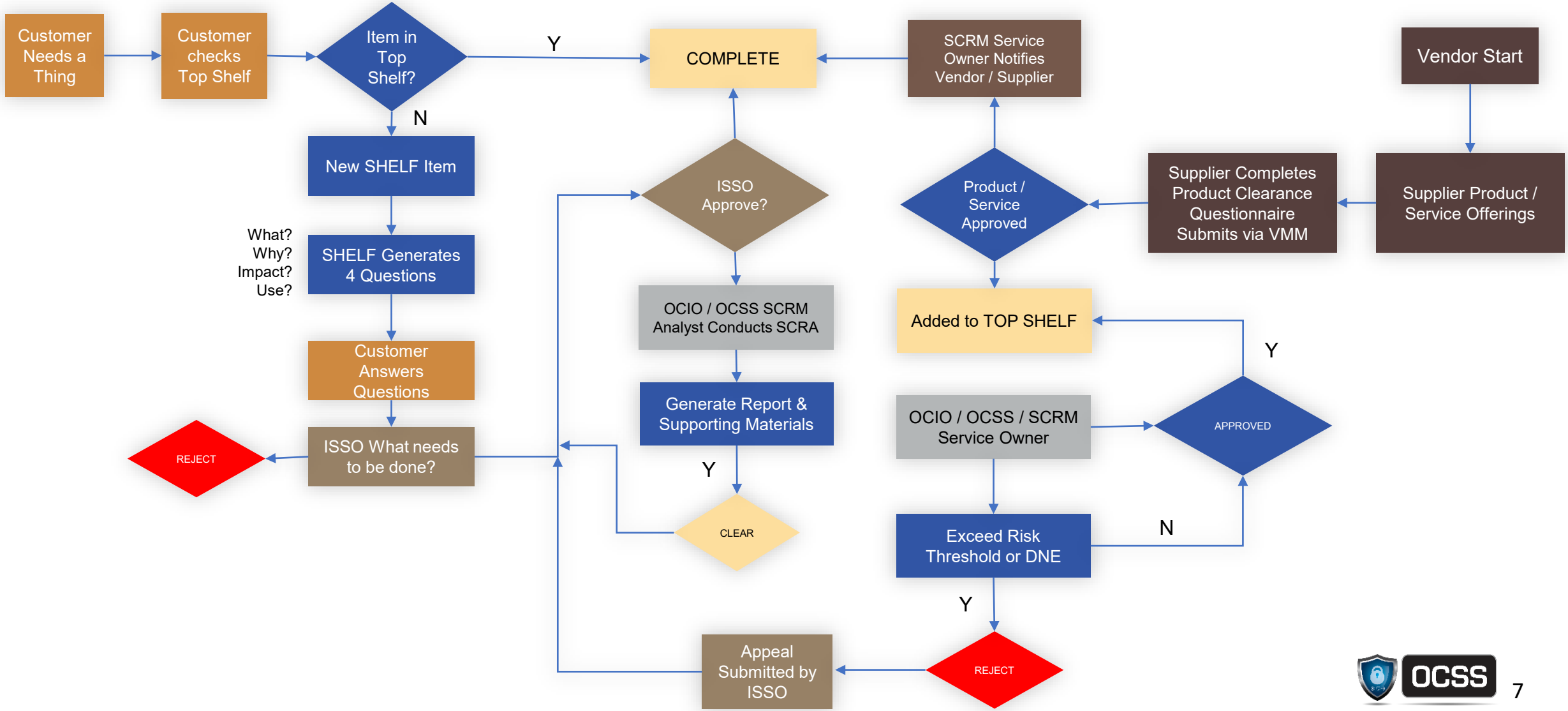
Circle of Trust: Internal Collaboration
Cross-functional group that understands threat vectors, system and/or component acquisition risk to the NASA environment and develop risk mitigation strategies.

4 **NASA OCIO/OCSS**
Makes final determination to clear item based on assessment. If cleared, item is added to the ACL and notification is sent to ITAMs, Center POC and initiating customer. This is **NOT** an authorization to purchase. If not cleared, ITAMs, Center POC and initiating customer are notified of final decision and may pursue an appeal.



5 **Agency ITAMS**
Facilitates the acquisition of the product/service. [NF1707]

SCRM Future State: Proactive Supplier Engagement Process (PSEP)



Introductory Briefing

1 Introductory Briefing

Questionnaire Completion

1 Introductory Briefing

2 Questionnaire Completion

Questionnaire Response Review

1 Introductory Briefing

2 Questionnaire Completion

3 Questionnaire Response Review

Entity Briefing & Discussion

1 Introductory Briefing

2 Questionnaire Completion

3 Questionnaire Response Review

4 Entity Briefing & Discussion

Internal CoT Briefing

1 Introductory Briefing

2 Questionnaire Completion

3 Questionnaire Response Review

4 Entity Briefing & Discussion

5 ICT SCRM Service Owner Briefing to Internal CoT

Final Decision

1 Introductory Briefing

2 Questionnaire Completion

3 Questionnaire Response Review

4 Entity Briefing & Discussion

5 ICT SCRM Service Owner Briefing to Internal CoT

6 Final Decision

Inclusion in NASA's Catalog

1 Introductory Briefing

2 Questionnaire Completion

3 Questionnaire Response Review

4 Entity Briefing & Discussion

5 ICT SCRM Service Owner Briefing to Internal CoT

6 Final Decision

7 Inclusion in NASA's Catalog

Continuous Monitoring & Collaboration

1 Introductory Briefing

2 Questionnaire Completion

3 Questionnaire Response Review

4 Entity Briefing & Discussion

5 ICT SCRM Service Owner Briefing to Internal CoT

6 Final Decision

7 Inclusion in NASA's Catalog

8 Continuous Monitoring & Collaboration

Key PSEP Objectives

1

Collect Once; Share Many

Portfolios are used to compare different risk perspectives within a company. They are used to group suppliers in order to easily compare them with each other.

2

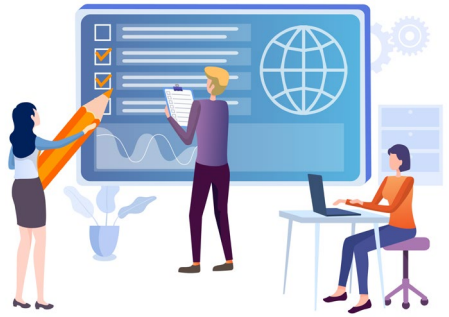
Risk Assessment

An analysis of publicly available information about suppliers. They contain an Executive Summary, Corporate Overview, Risk Summary, Risk Narratives, and Analyst Comments.

3

Risk Factor Narrative

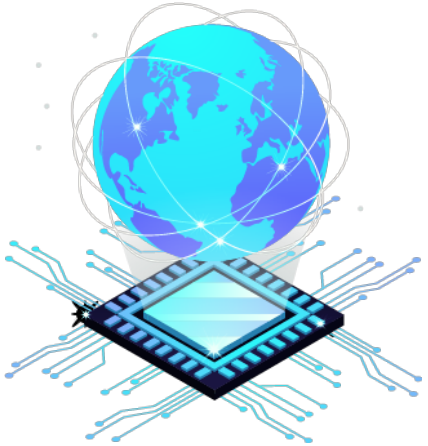
An in-depth description of the sources of the risk for that Risk Factor.



4

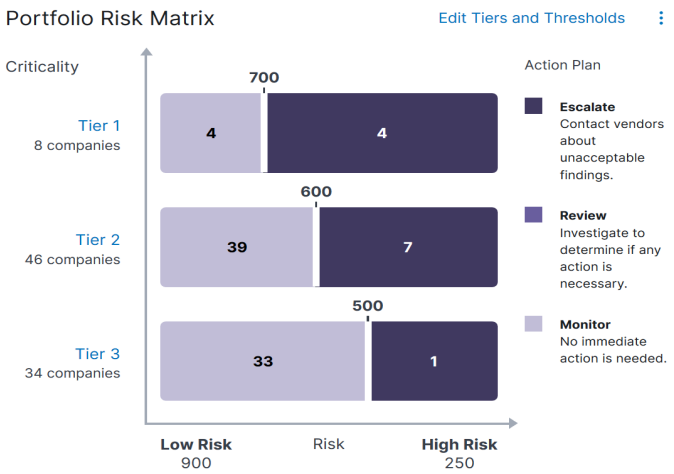
Eco-System Mapping

Eco-System mapping refers to how we are identifying, categorizing, and visually representing relationships between entities.

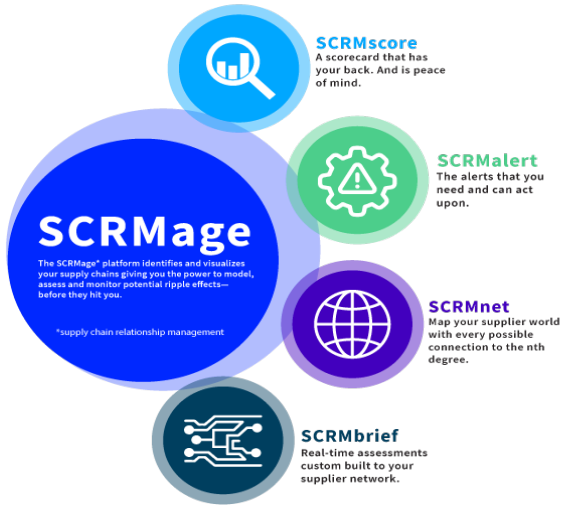


NASAs ICT SCRM Toolkit

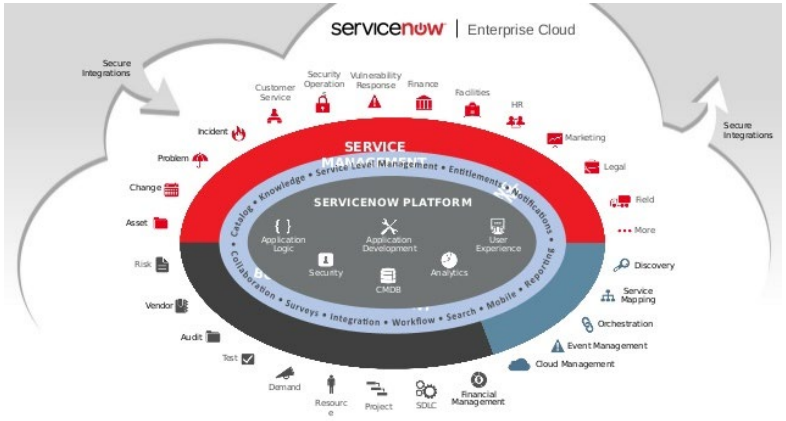
BITSIGHT
The Standard in SECURITY RATINGS



interos

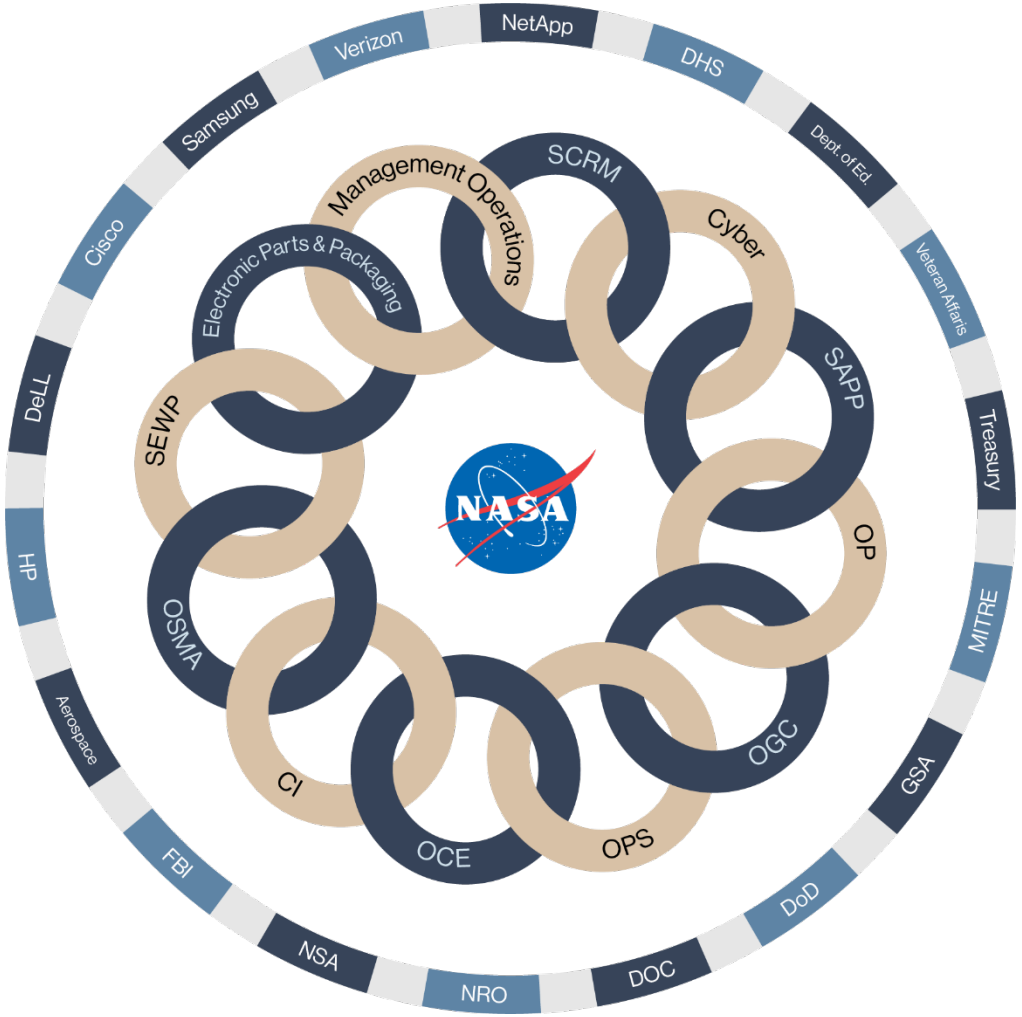


MVISION



OCSS

NASA's Circle of Trust & Partnerships



Q & A

Kanitra D. Tyler

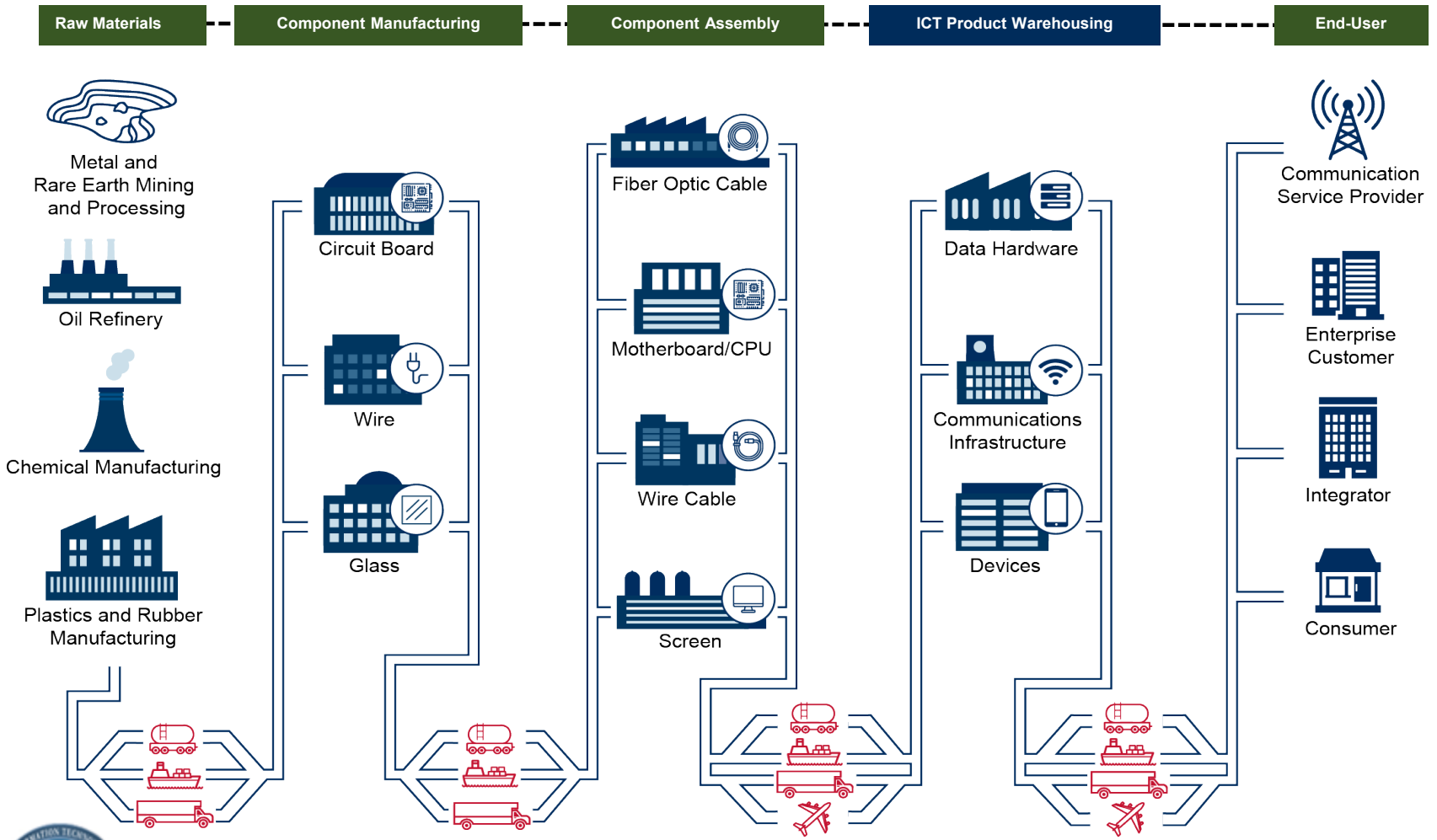
CISSP, CAP, CEH, NSA IAM/IEM, CHFI, CECS, ITIL v3
Supply Chain Risk Management Service Owner (SCRM) | NASA

Office of Cybersecurity Services (OCSS)
Office of the Chief Information Officer (OCIO)
301.286.6173 – phone
301.286.4262 – fax
240.472.3371 – cell
SIPR Email: kanitra.tyler@nss.sgov.gov
JWICS Email: kanitra.tyler@nasa.ic.gov
vIPer: 240-684-9053 (secure phone)

Questions?

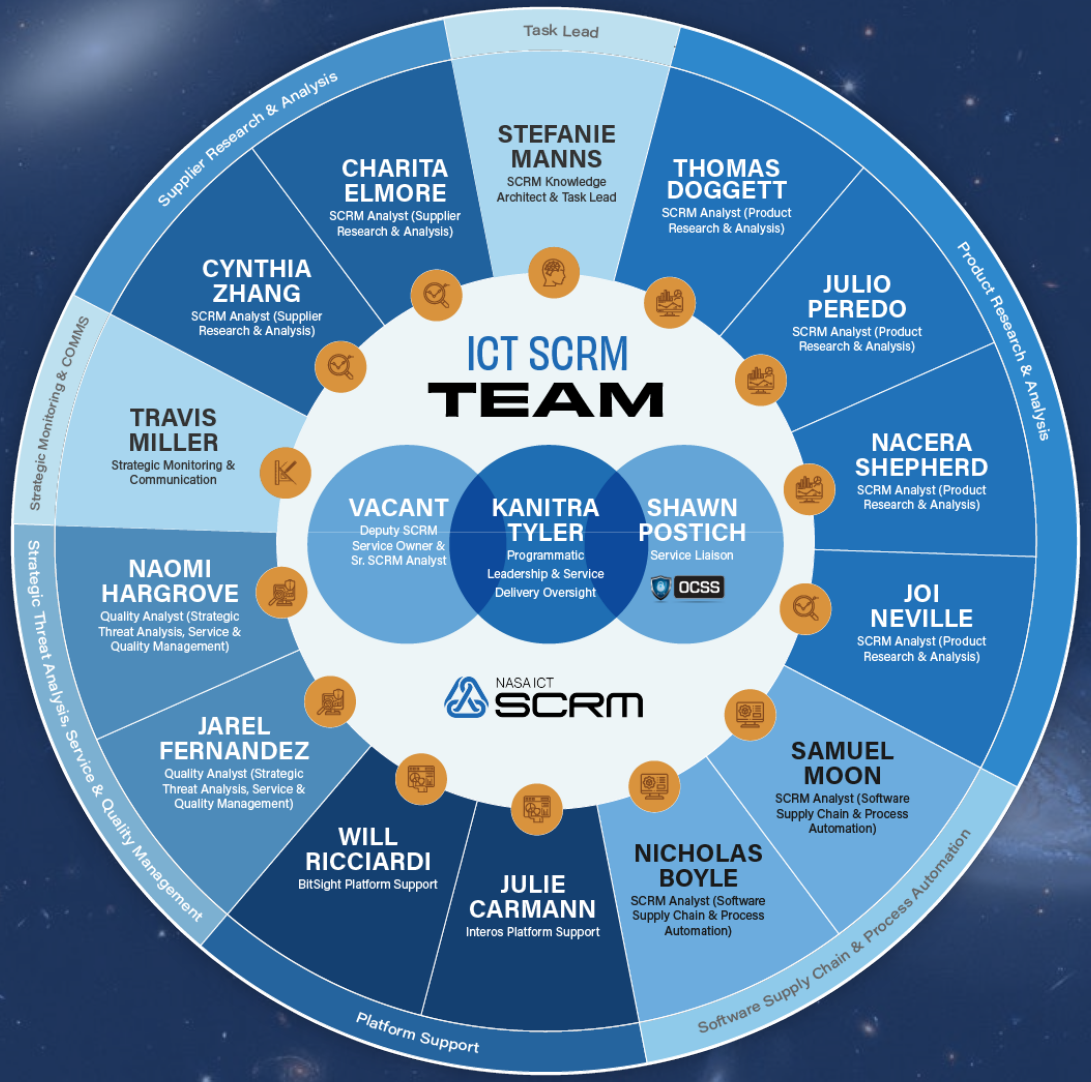
Back-up & References

What is a Supply Chain (SC)



ICT Supply Chain System Map

NASA's ICT SCRM Team & Functions

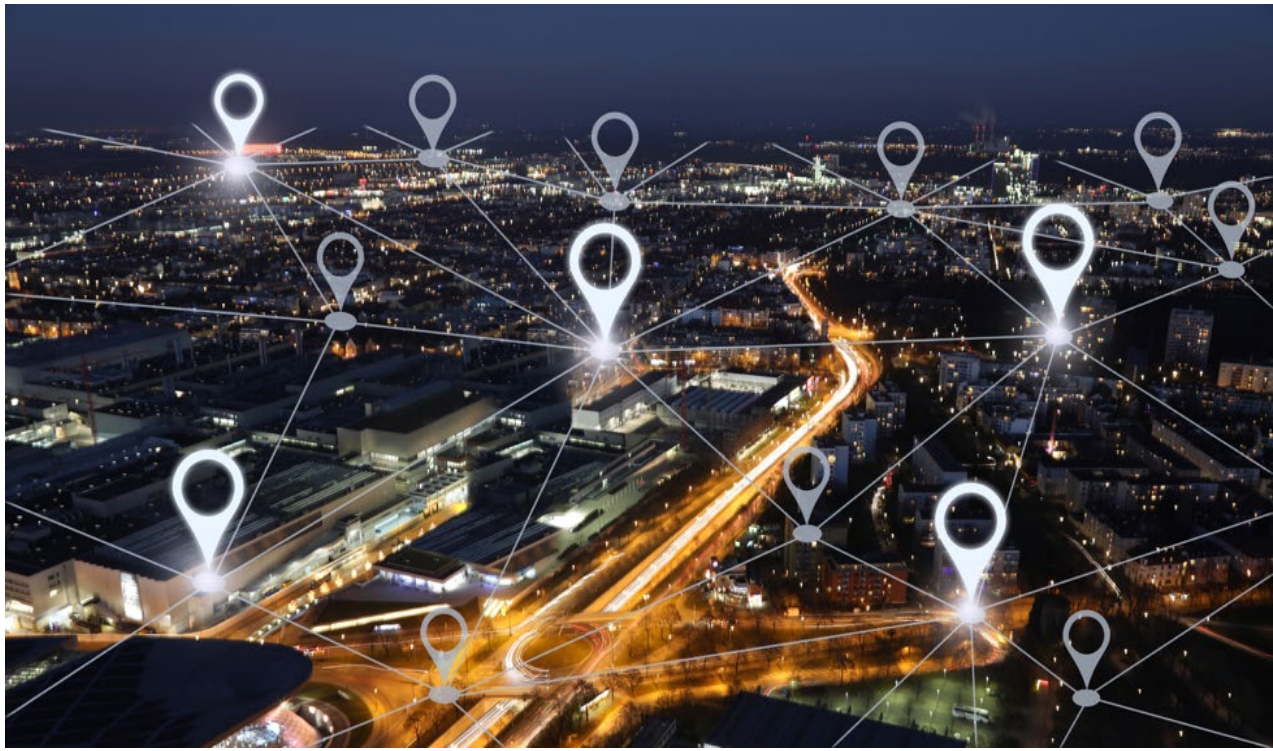


Functions

- Programmatic Leadership & Service Delivery Oversight
- Knowledge Architect & Task Leadership
- Supplier Research & Analysis
- Product Research & Analysis
- Software Supply Chain & Process Automation
- Strategic Threat Analysis, Service & Quality Management
- Strategic Monitoring & Communication

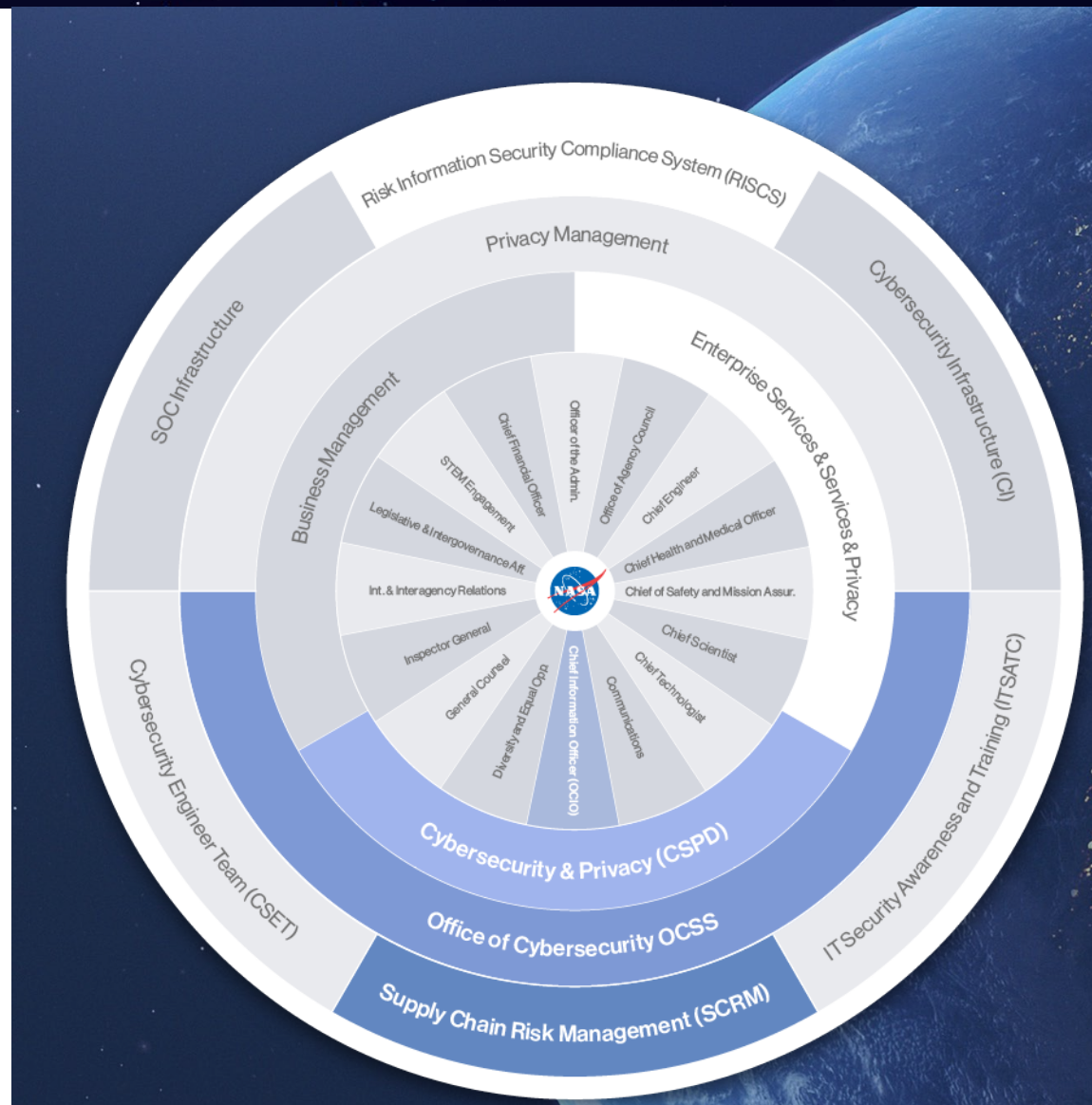
The Three P's of NASA ICT SCRM

- 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



ICT SCRM Service Governance Structure

ICT SCRM is an **Enterprise Shared Service Solution** delivered from Goddard Space Flight Center (GSFC)



Federal Drivers

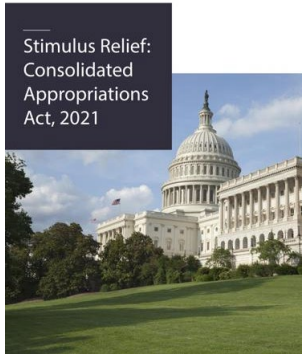
OMB A-130
Management of Federal Information Resources - 1985-2016

FISMA
Federal Information Security Modernization Act - 2014

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

ICD 731 Supply Chain Risk Management for the Intelligence Community

S.1388 – Supply Chain Counterintelligence (CI) Training Act of 2019
To manage supply chain risk through CI. training, and for other purposes.



Consolidated Appropriations Act, 2021, Secs. 208 & 514
Issued by Congress requiring Federal agencies to perform risk assessments for acquisition of Moderate – or High-Impact systems.

John S. McCain National Defense Authorization Act for Fiscal Year 2019
Authorizes FY19 appropriations and sets forth policies regarding the military activities of DoD as well as sections being adopted in the FAR.

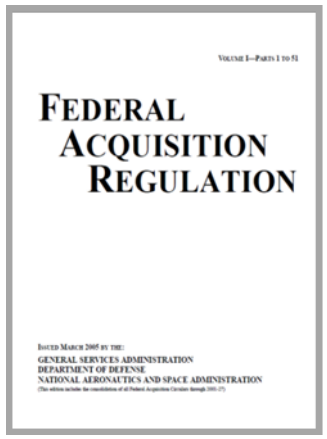
NIST: Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028
Publishing guidance that outlines security measures for critical software use.

NIST SP 800-37 Rev 2:
Guide for Applying the Risk Management Framework to Federal Information Systems

NIST SP 800-53 Rev 5:
Security and Privacy Controls for Federal Information Systems and Organizations

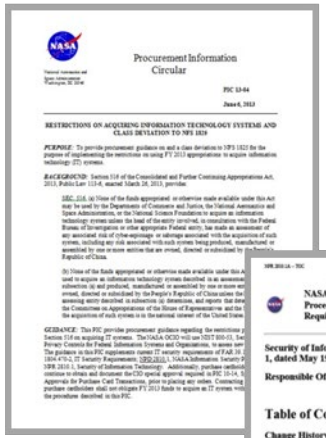
NIST 800-60 V1R1:
Guide for Mapping Types of Information and Information Systems to Security Categories

NIST SP 800-161 Rev 1:
Supply Chain Risk Management Practices for Federal Information Systems and Organizations

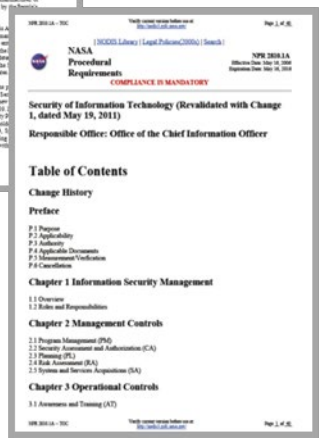


FAR Guidance
Issued by the General Services Administration, the Dept. of Defense, and NASA

Federal Acquisition Supply Chain Security Act (FASCA)
Issued by Federal Acquisition Security Council (FASC)



Procurement Class Deviation 15-03D:
(January 13, 2020) (Sept. 11, 2018)
Implements Consolidated Appropriations Acts



NPR 2810.1:
NASA Procedural Requirements: Security of Information Technology

EXP: Oct. 16, 2021

Applicable Cyber Supply Chain Executive Orders

PRESIDENTIAL ACTIONS

February 12, 2013

EO 13636 Improving Critical Infrastructure Cybersecurity

May 15, 2019

EO 13873 Securing the Information and Communications Technology and Services Supply Chain

April 4, 2020

EO 13913 Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector

January 19, 2021

EO 13984 Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities

January 25, 2021

EO 14005 Ensuring the Future Is Made in All of America by All of America's Workers

February 24, 2021

EO 14017 America's Supply Chains

April 15, 2021

EO 14024 Blocking Property with Respect to Specified Foreign Activities of the Government of the Russian Federation

May 12, 2021

EO 14028 Improving the Nation's Cybersecurity

June 9, 2021

EO 14034 Protecting Americans' Sensitive Data from Foreign Adversaries

Applicable Supply Chain Memoranda

MEMORANDA

August 27, 2021 | M-21-31

Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents

June 11, 2021 | M-21-26

Increasing Opportunities for Domestic Sourcing and Reducing the Need for Waivers from Made in America Laws

July 20, 2020 | M-20-28

Buying for America

August 10, 2021 | M-21-30

Protecting Critical Software Through Enhanced Security Measures

November 9, 2020 | M-21-02

Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements

December 10, 2018 | M-19-03

Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program

Resources

- Executive Order on America's Supply Chains
- Executive Order on Improving the Nation's Cybersecurity
- CISA ICT SCRM Task Force
- CISA Software Bill of Materials (SBOM)
- NIST's Responsibilities under the Executive Order
  - NIST Critical Software Definition & Explanatory Material