Raytheon Technologies

NDIA Systems & Mission Engineering Conference 2021

Cyber Supply Chain Risk Management (SCRM) Engineer, a Security Specialty within System Security Engineering

Abstract #23774

Holly Dunlap, Holly.Dunlap@Raytheon.com
Raytheon Missiles & Defense, System Security Engineering
Cyber SCRM Engineering SME

December 2021

Distribution Statement A- Approved for public release; distribution is unlimited.

© 2021 Raytheon Technologies Corporation.
All rights reserved.

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Agenda

- What is Cyber SCRM?
- Adversary
- Global Supply Chain Risks
- Customer Requirements
- Standards
- Future State Vision
- Integrating Cyber SCRM into RTX – It's a journey.
- Raytheon Cyber SCRM Role & Responsibility
- Customer Program Perspective Example
- Key Takeaways

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Key Definitions

- **Supply Chain Risk.** The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.
  - DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

- ***Cyber Supply Chain Risk Management*** **(C-SCRM)** is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of ICT product and service supply chains. It covers the entire lifecycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction) as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an ICT product or service at any stage of the lifecycle. Department Homeland Security (DHS)

- ***Cyber Supply Chain Risk Management (C-SCRM)*** is a systematic process for managing cyber supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and developing response strategies to the cyber supply chain risks presented by the supplier, the supplied products and services, or the supply chain.
  - *DRAFT* NIST 800-161 Rev 1, Cyber Supply Chain Risk Management Practices for Systems and Organizations

* ICT – Information Communication Technology

Distribution Statement A- Approved for public release; distribution is unlimited.

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

The Threat is Real…

The Adversary has moved from attacking our systems directly to attacking our supply chain.

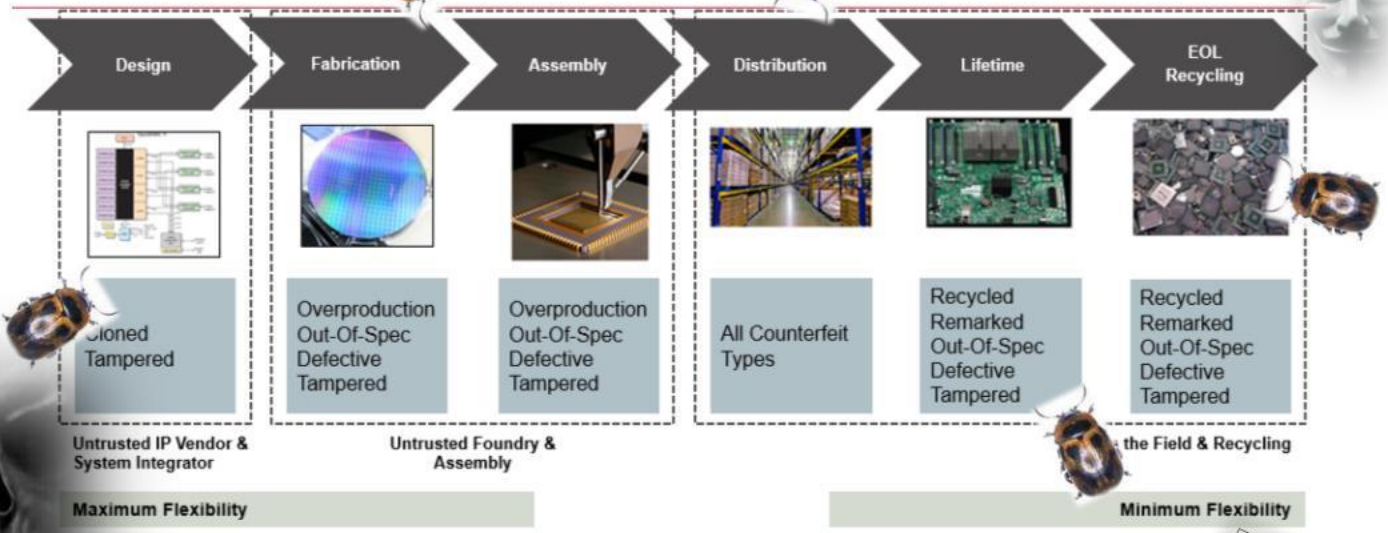
Battlefield Losses: Yugoslav Museum of Aviation

These are *Not* Cooperative R&D Efforts

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Cyber Supply Chain Risk Management

The Global Supply Chain presents the greatest attack surface to our national security systems.



Microelectronics is DOD's new No. 1 technology priority,
bumping hypersonics to No. 3 – Inside Defense June 29, 2020

We are responsible the authenticity & integrity of the components integrated into our systems.

Raytheon Technologies

Distribution Statement A- Approved for public release; distribution is unlimited.

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Key Protection Activities to Improve Cyber Resiliency

Cyber SCRM Requirements are derived from DoDI 5200.44

Program Protection & Cybersecurity

DoDI 5000.02, Enclosure 3 & 14

DoDM 5200.01, Vol. 1-4 | DoDM 5200.45 | DoDI 8500.01

DoDI 5200.39 | DoDI 5200.44 | DoDI 5230.24 | DoDI 8510.01

Technology

What: A capability element that contributes to the warfighters' technical advantage (CPI)

Key Protection Activity:

- Anti-Tamper
- Defense Exportability Features
- CPI Protection List
- Acquisition Security Database

Goal: Prevent the compromise and loss of CPI

Components

What: Mission-critical functions and components

Key Protection Activity:

- Software Assurance
- Hardware Assurance/Trusted Foundry
- Supply Chain Risk Management
- Anti-counterfeits
- Joint Federated Assurance Center (JFAC)

Goal: Protect key mission components from malicious activity

Information

What: Information about the program, system, designs, processes, capabilities and end-items

Key Protection Activity:

- Classification
- Export Controls
- Information Security
- Joint Acquisition Protection & Exploitation Cell (JAPEC)

Goal: Ensure key system and program data is protected from adversary collection

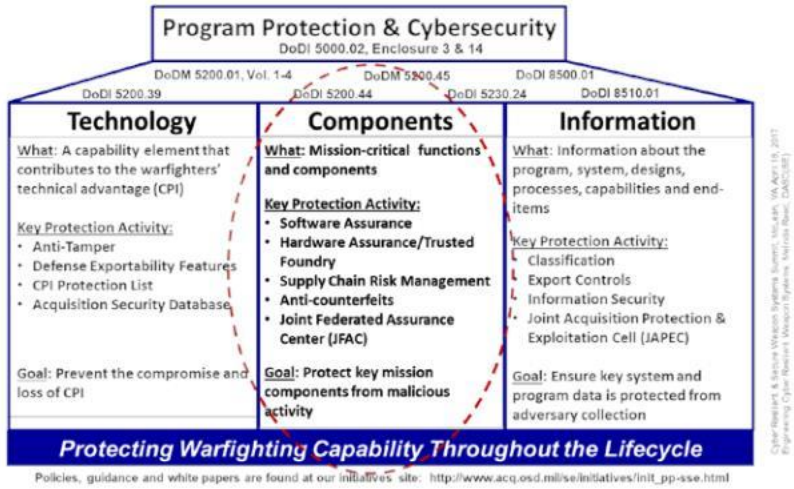
Protecting Warfighting Capability Throughout the Lifecycle

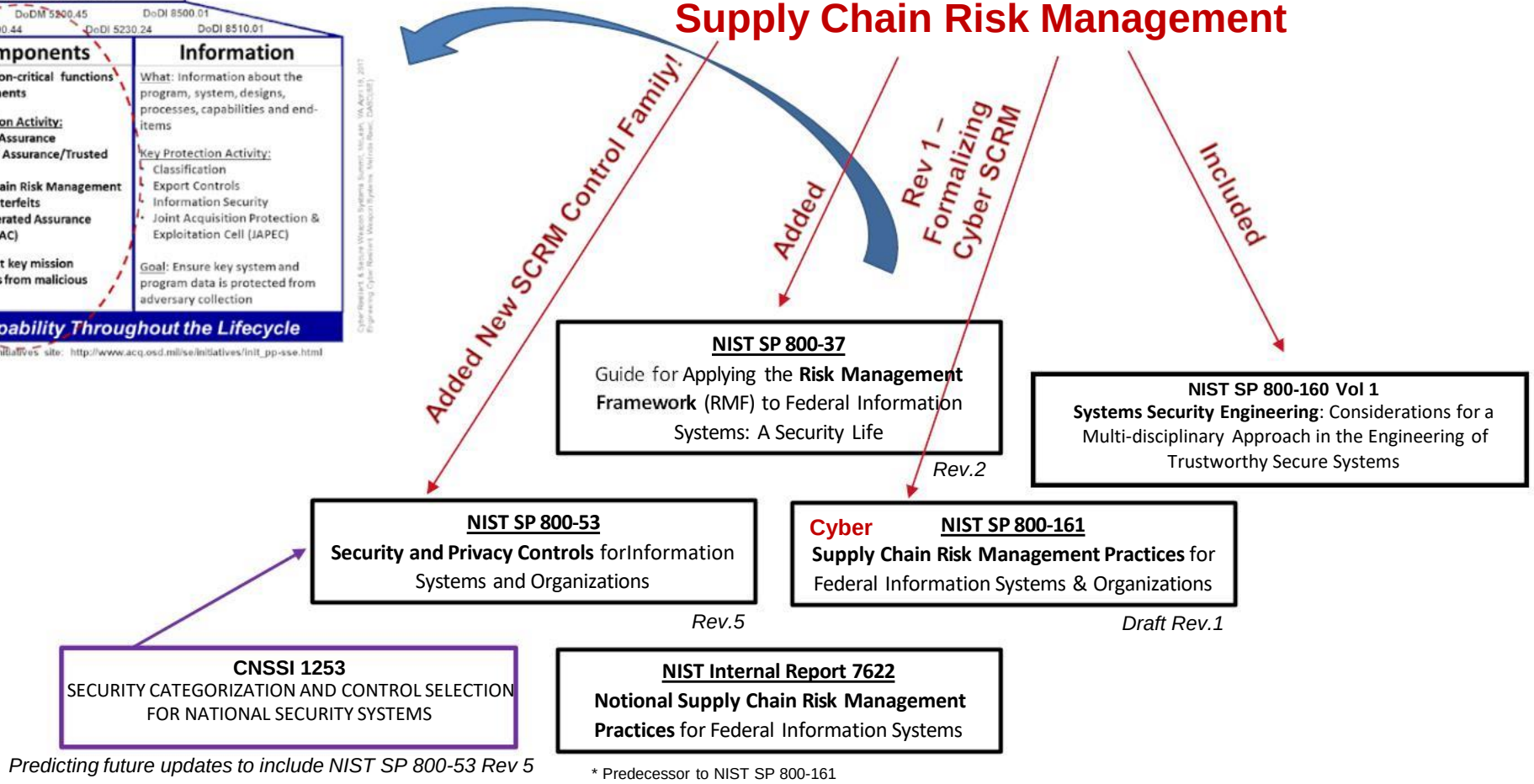
Cyber Resilient & Secure Weapon Systems Summit, McLean, VA April 18, 2017
Engineering Cyber Resilient Weapon Systems, Melinda Reed, DASD(SE)

Policies, guidance and white papers are found at our initiatives site: http://www.acq.osd.mil/se/initiatives/init_pp-sse.html

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Relationship of DoD Acquisition Policies and Industry Best Practices often referred to as Standards





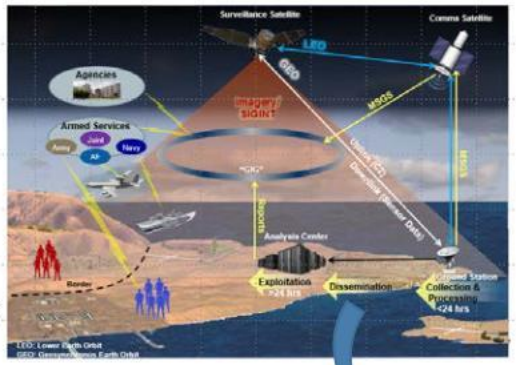
Distribution Statement A- Approved for public release; distribution is unlimited.

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

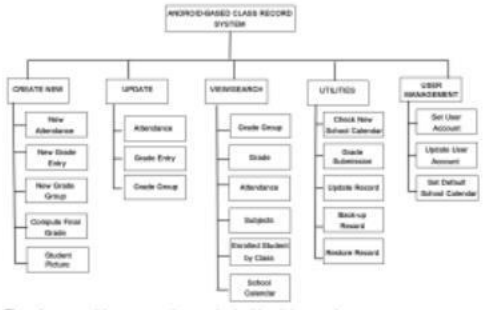
Raytheon Future State
Cyber Supply Chain Risk Management

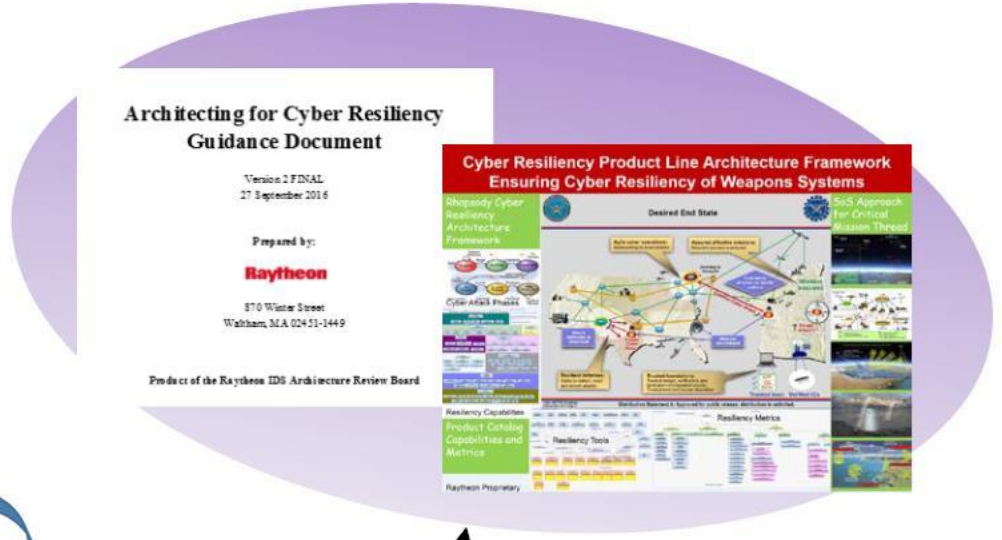
Operational Systems of Systems

Mission Thread Analysis to Critical Component Identification & Categorization Enabler



System Functional Decomposition





SwA Raytheon Vulnerability Assessment Process (Guide & Enabler)

Internal Test Capability Catalog & Guide

Capability 1,2,3,4,5….
- Applicable Type of Component
- Level of Risk Mitigation

Statistical Test Optimization

Software / Firmware (?)

Hardware / Firmware

Test

Critical Components Identification & Categorization (Hardware, Software, Firmware)

Architecture Design Testing

Internal

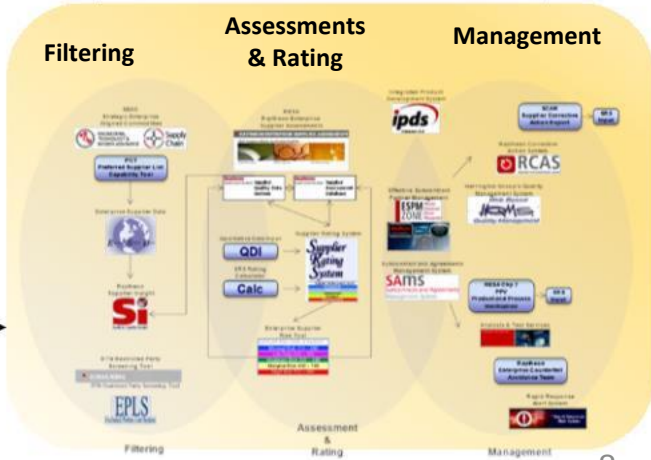
Internal Or External

External

Internal Risk Mitigation Product Catalog

Supply Chain Trade Space Options

Filtering | Assessments & Rating | Management



Raytheon Technologies

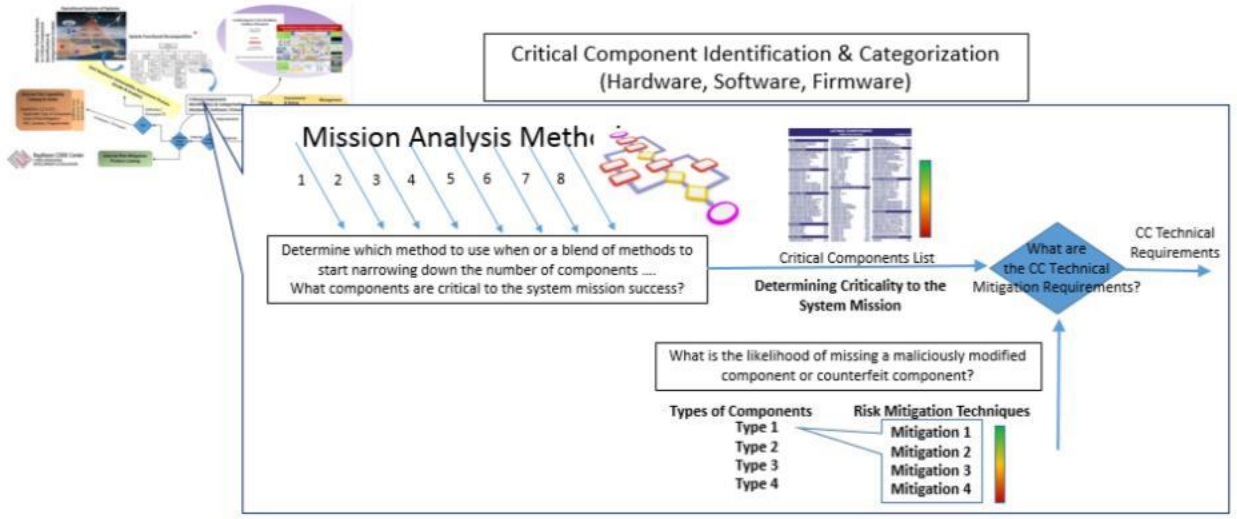
Distribution Statement A- Approved for public release; distribution is unlimited.

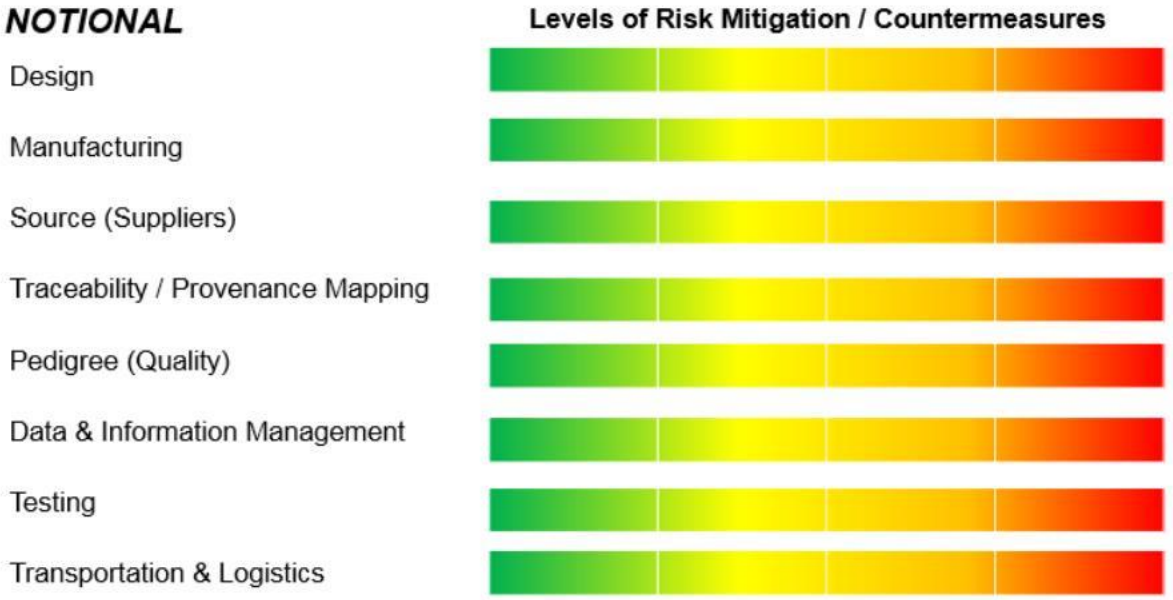
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Catalog Trade Based Cyber SCRM Options

Programs need a ***range of risk mitigations*** to address supply chain risks for our System Mission Critical Components.

- Tiered Component Design Features
- Tiered Criteria and Audits for Levels of Security in Manufacturing
- Tiered Criteria and Evaluation of Suppliers
- Tiered Criteria for Critical Component Pedigree
- Tiered Requirements to Flow to Suppliers for How to Manage Data & Information
- Tiered Criteria and Options for Test Requirements and Evidence by the Type of Component
- Tiered Criteria and Options for Transportation & Logistics Mitigations.





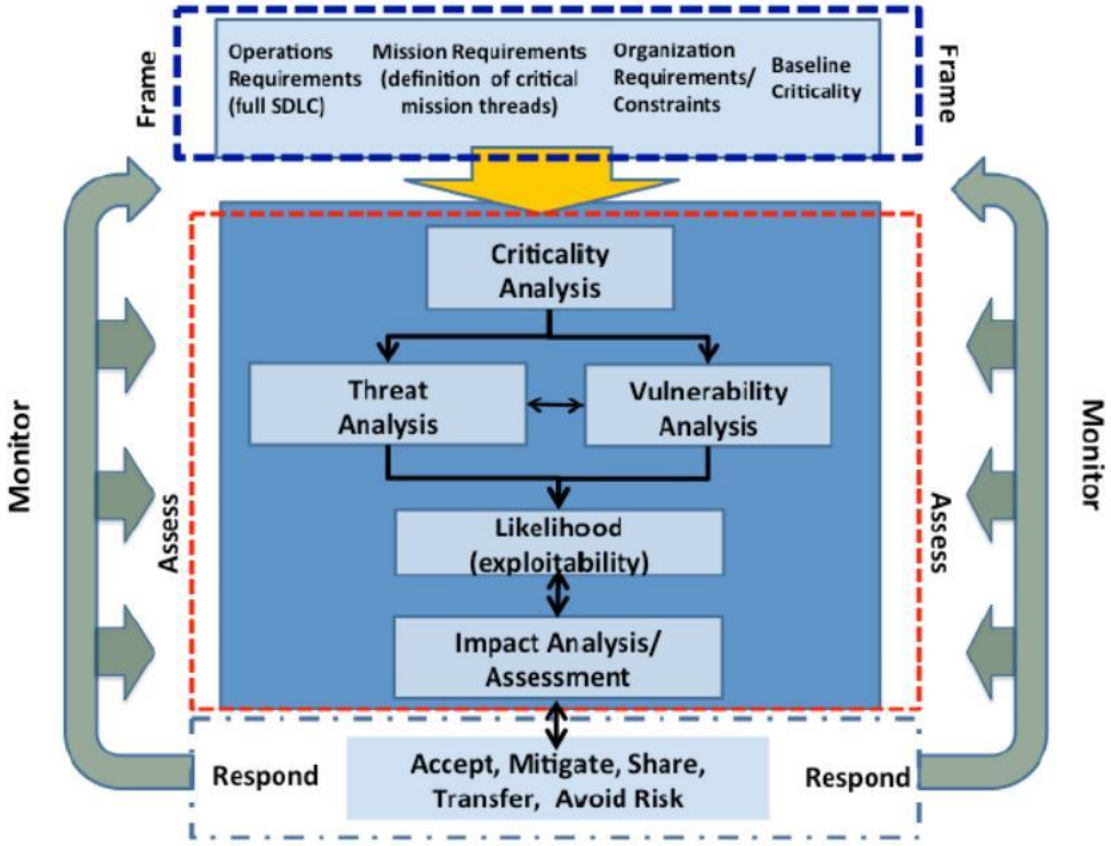
Raytheon Technologies

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

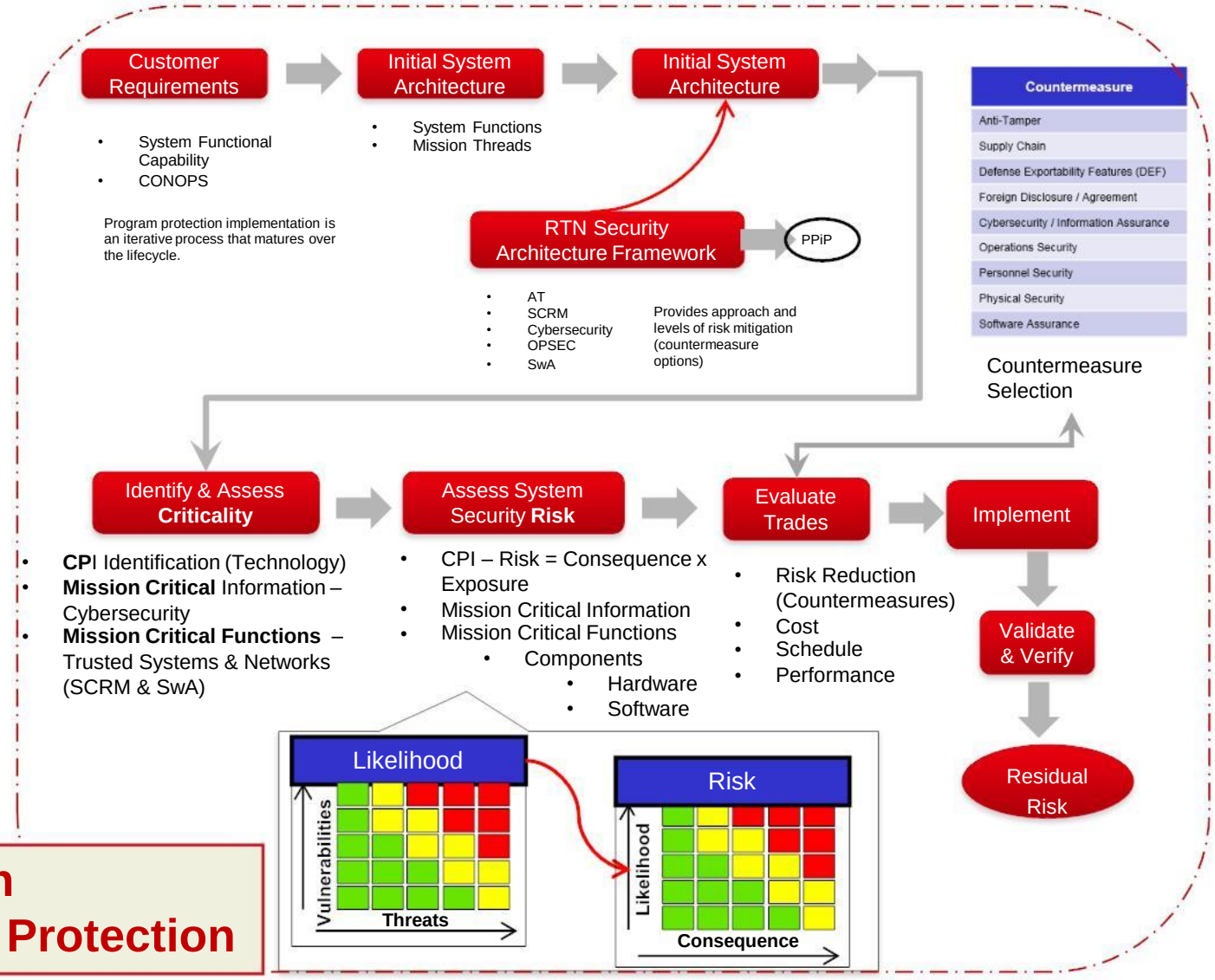
Cyber Supply Chain Risk Management

NIST SP 800-161

Supply Chain Risk Management Practices for Federal Information Systems & Organizations



https://csrc.nist.gov/publications/detail/sp/800-161/final

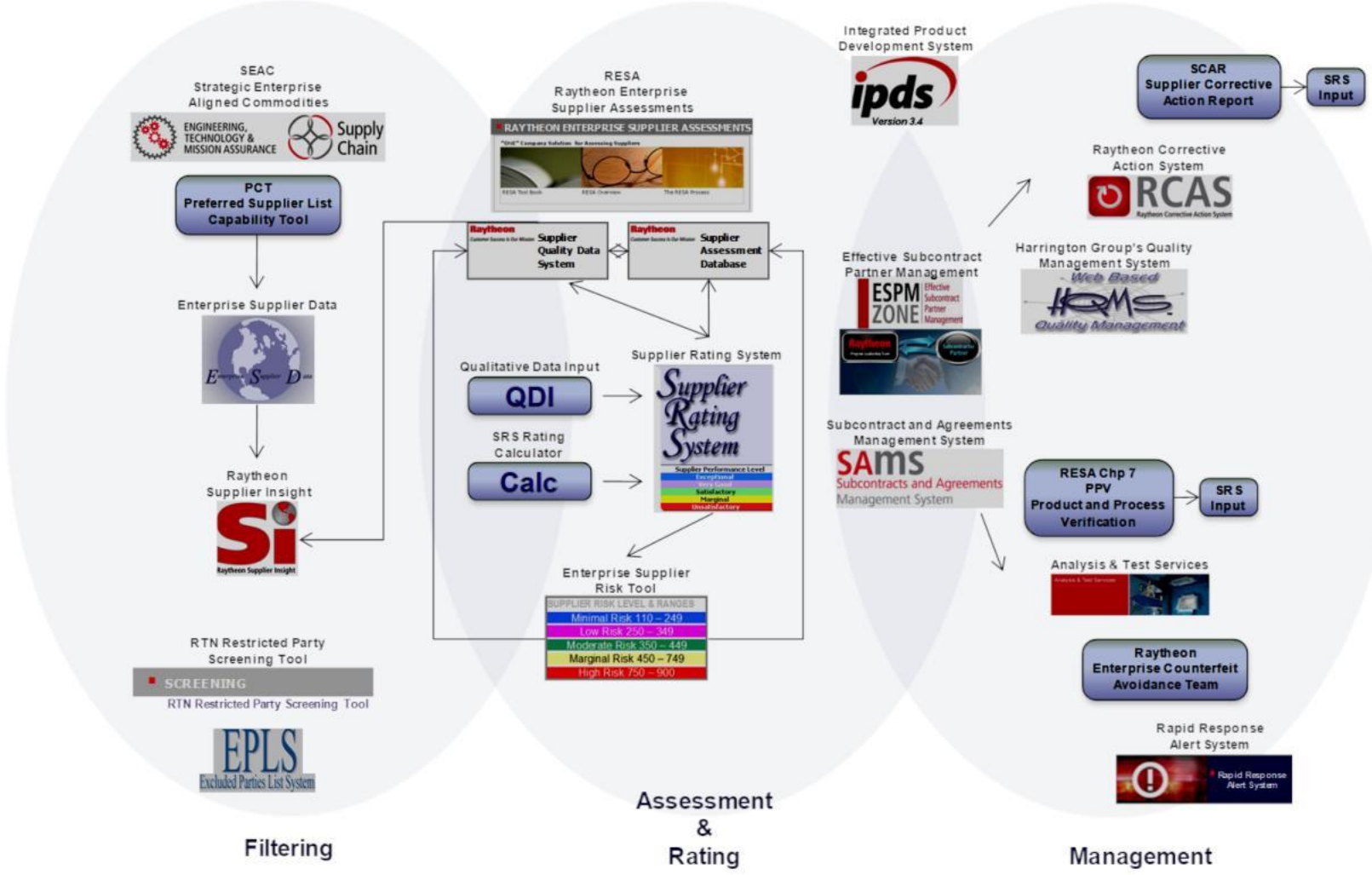


Raytheon Program Protection

Raytheon Technologies

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

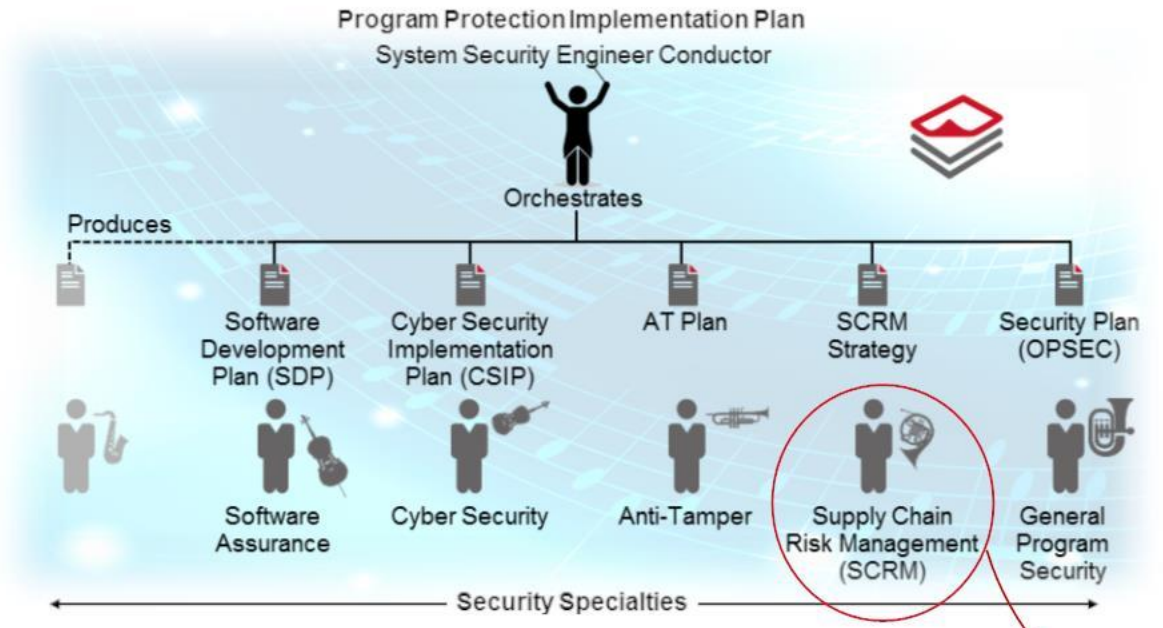
Raytheon's Integrated Supply Chain Construct

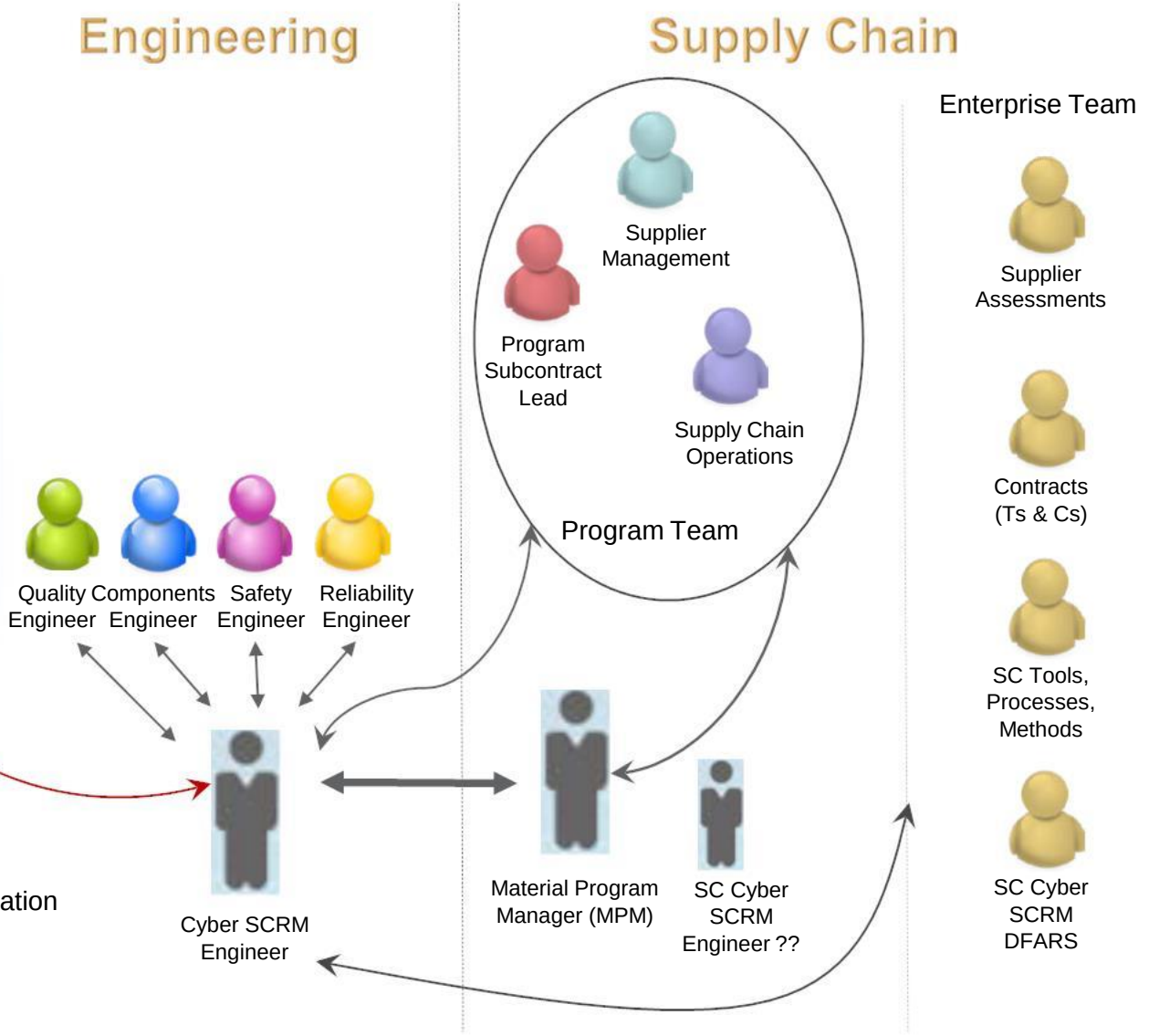


Integrate Cyber SCRM Considerations into Existing Raytheon Supply Chain Methods and Tools

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Raytheon's Cyber SCRM Role OV-1





The Cyber SCRM Engineering Lead is responsible for the program strategy and technical subsystem and component procurement and subcontracting requirements to address global supply chain risks.

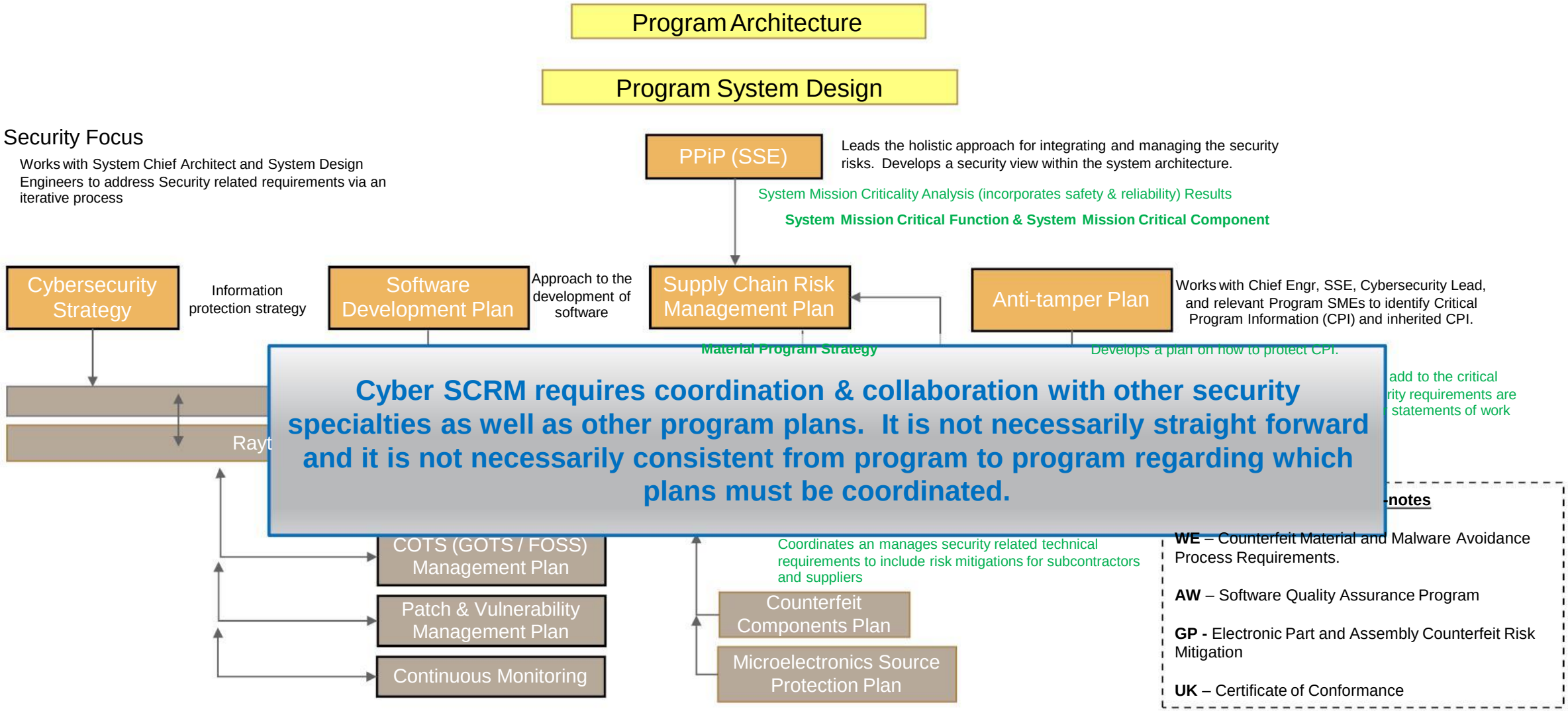
- Cyber SCRM Strategy
- System Mission Criticality Analysis for Logic Bearing Critical Component Identification
- Bill of Materials Decomposition
- Mitigation Evaluation for Procured and Subcontracted Material and Software.
- Supplier / Sub Selection Criteria for Cyber SCRM Considerations
- Cyber SCRM Asset Management Considerations

Cyber SCRM Engineer Addresses Global Supply Chain Risks to Program Procurements

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Example Raytheon Program Cyber SCRM Perspective

Holly Dunlap



Raytheon's Cyber Supply Chain Risk Management Program Plan Relational Mapping

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Cyber Supply Chain Risk Management
Key Takeaways

- Adversaries are moving from directly attacking our systems to attacking our more vulnerable supply chains.
- Cyber SCRM is a new and developing security specialty discipline within System Security Engineering and Systems Engineering
- A partnership between Engineering, Mission Assurance, and Supply Chain organizations is an imperative.
- Cyber SCRM contributes to a holistic approach to program protection and a Program Protection implementation Plan (PPiP).

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

References:

- DoDI 5200.44
  - https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf?ver=2018-11-08-075800-903
- NIST SP 800-53 Rev 5
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
- NIST SP 800-160
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf
- NIST SP 800-161
  - https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft
- Deliver Uncompromised, A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War
  - https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-26AUG2019.pdf

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Questions?

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Holly Dunlap Bio

- BS Electrical Engineering & MBA
- 10 years Nuclear Weapons, National Nuclear Security Administration (NNSA) Kansas City Plant, M&O Honeywell
  - 3 Year Rotational Leadership Development Program (10 years experience in 3 years)
    - Program Manager of B83
    - Supply Chain 18 months (Rotated every 3 months)
    - Intelligence Community (Reverse Engineering, Rapid Fielding, Analysis)
  - Certified 6 Sigma Black Belt – Microelectronics
- OSD DDR&E Technical Intelligence, Pentagon +4 years
  - Emerging & Disruptive Technology. Investment strategy to ensure US technical capability advantage. Work intimately with Anti-tamper Executive Agent, National & Defense Intelligence Community, and Defense System Developers. Strategic 15 – 20 Year Planning.
- Ktech Later Acquired by RTN RMS
  - USD(I) Contract Supply Chain & Logistics Layered Analysis; Data & Information Exploitation. 18 month effort.
- RMS – IDS – RMD (+15 years)
  - NDIA System Engineering Division Elected Chair (+13 Committees, +500 members; government, industry, academia, FFRDC)
  - NDIA System Security Engineering Committee Chair, +9 years
  - Raytheon Systems Engineering Council – Cyber Resiliency & System Security Project Lead
  - Cyber Enterprise Campaign
  - Cyber Operations Development & Evaluation (CODE) Center
  - PI Security & Trustworthy Foundations for Electronics Resurgence (STryFER) IDIQ Contracted Research & Development (CRAD) Proposal

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Thank you.

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.