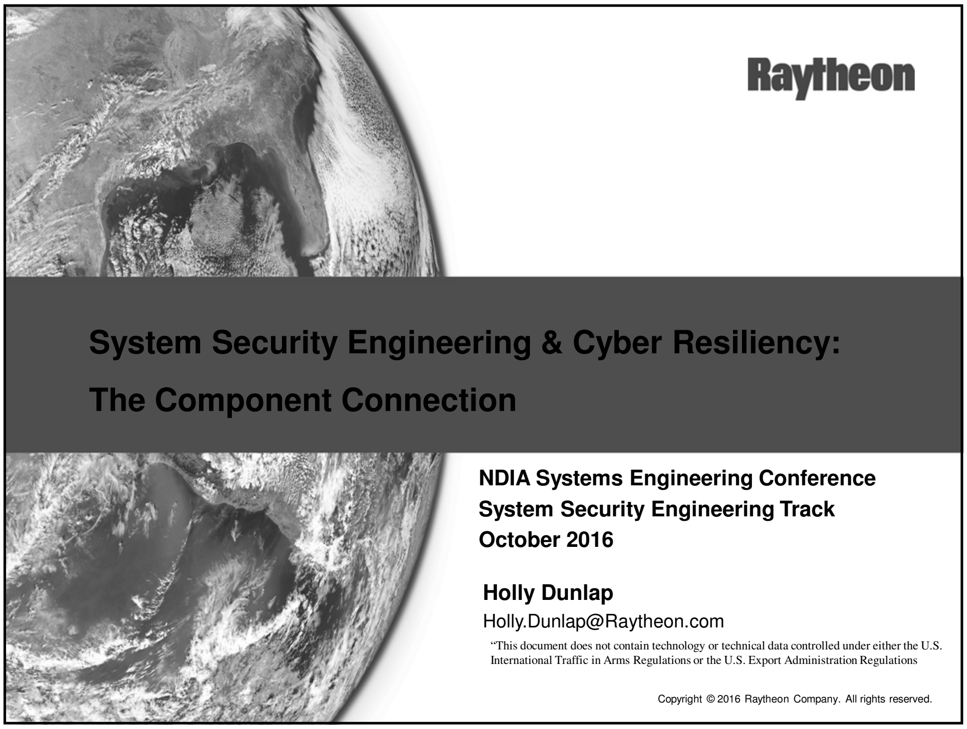


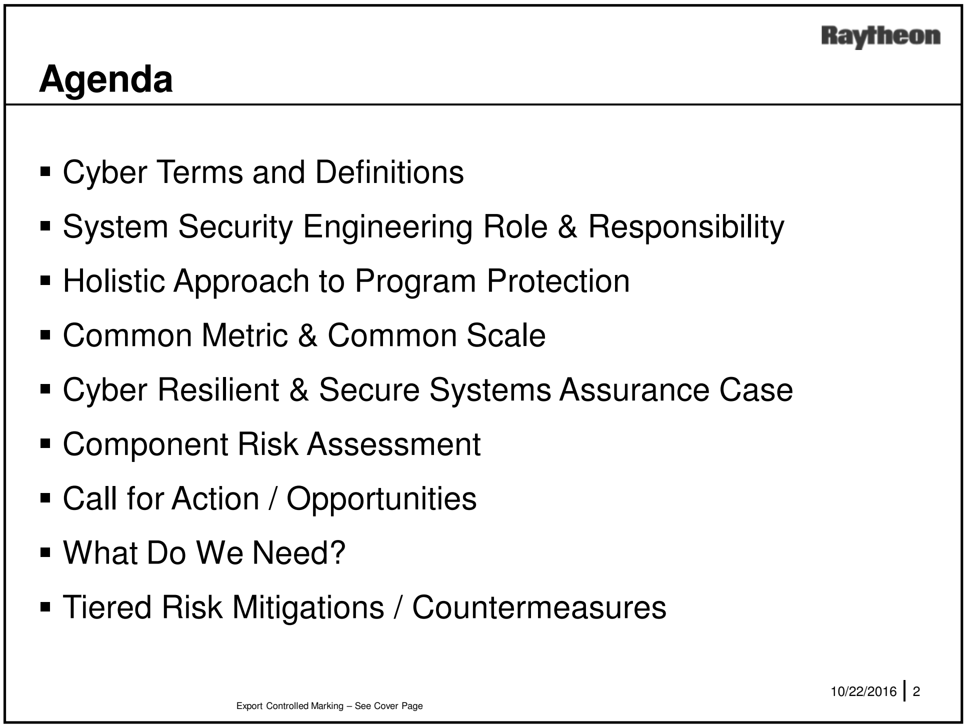
Raytheon

System Security Engineering & Cyber Resiliency: The Component Connection

NDIA Systems Engineering Conference
System Security Engineering Track
October 2016

Holly Dunlap
Holly.Dunlap@Raytheon.com

"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

Agenda

- Cyber Terms and Definitions
- System Security Engineering Role & Responsibility
- Holistic Approach to Program Protection
- Common Metric & Common Scale
- Cyber Resilient & Secure Systems Assurance Case
- Component Risk Assessment
- Call for Action / Opportunities
- What Do We Need?
- Tiered Risk Mitigations / Countermeasures

Export Controlled Marking – See Cover Page

Raytheon

What is Cyber Resiliency?

- Cyber resilience is the resilience of DoD systems to cyber attacks.
- *Cyber* is broadly used to address the components and systems that provide all digital information, including weapons/battle management systems, IT systems, hardware, processors, and software operating systems and applications, both stand-alone and embedded.
- *Resilience* is defined as the ability to provide acceptable operations despite disruption: natural or man-made, inadvertent or deliberate.
- *Operational resilience* is the ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions.

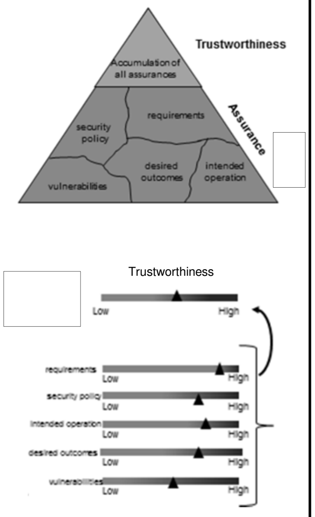
DoD Defense Science Board Task Force Report: Resilient Military Systems and Advanced Cyber Threat, January 2013, Cyber Resilience; DoDI 9500.01, Operational Resilience

Raytheon

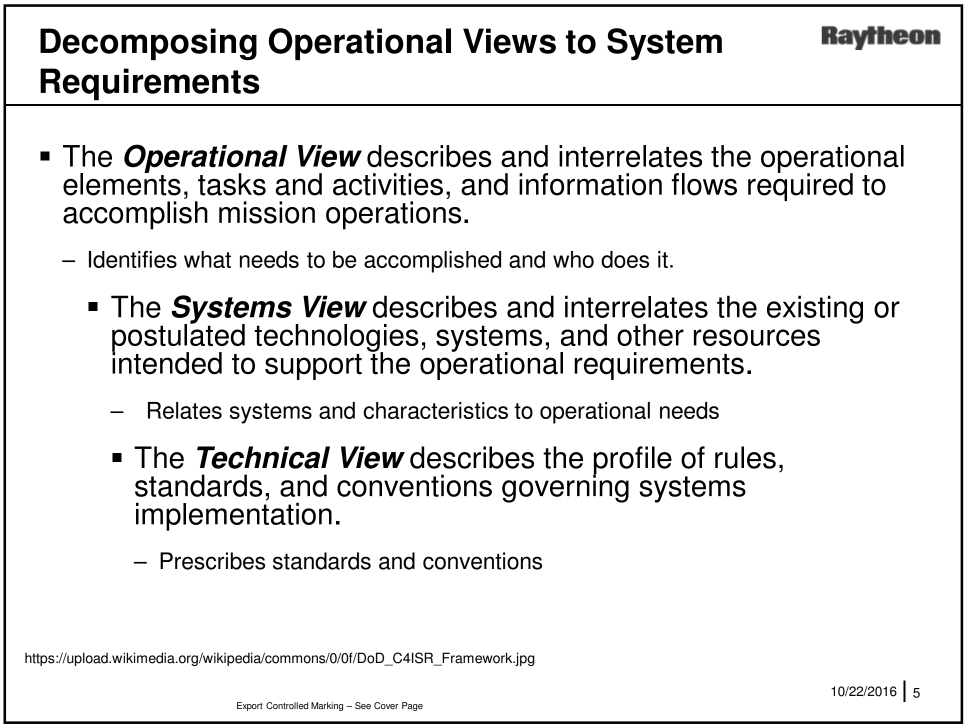
System Security Engineering

Systems security engineering is a specialty engineering discipline of systems engineering

- **Assesses susceptibility to threats** in the projected or actual environment of operation;
- **Identifies and assesses vulnerabilities** in a system and its environment of operation;
- **Identifies, specifies, designs, and develops protective measures** to address system vulnerabilities;
- **Identifies and evaluates protective measures** to ascertain their suitability, effectiveness and degree to which they can be expected to reduce mission/business risk;
- **Provides assurance evidence to substantiate the trustworthiness** of protective measures;
- **Identifies, quantifies, and evaluates the costs and benefits** of protective measures to inform **engineering trade-off and risk treatment decisions**; and
- **Leverages multiple security focus areas to ensure that protective measures are appropriate**, effective in combination, and interact properly with other system capabilities



Source: NIST SP 800-160 (Draft)

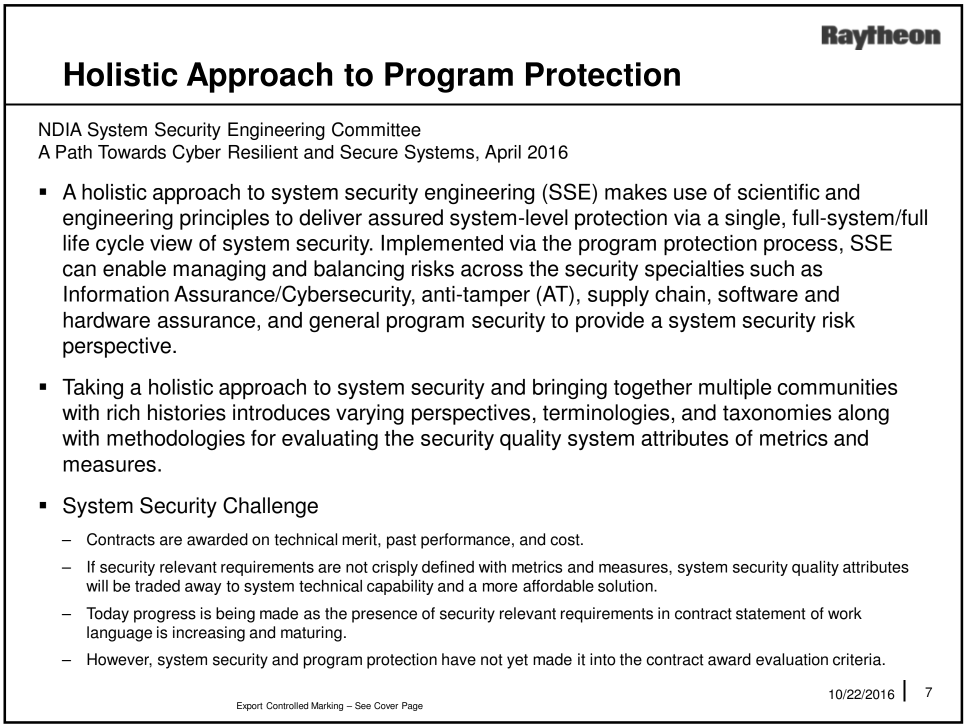


Decomposing Operational Views to System Requirements

Raytheon

- The ***Operational View*** describes and interrelates the operational elements, tasks and activities, and information flows required to accomplish mission operations.
  - – Identifies what needs to be accomplished and who does it.
  - The ***Systems View*** describes and interrelates the existing or postulated technologies, systems, and other resources intended to support the operational requirements.
    - – Relates systems and characteristics to operational needs
    - The ***Technical View*** describes the profile of rules, standards, and conventions governing systems implementation.
      - – Prescribes standards and conventions

https://upload.wikimedia.org/wikipedia/commons/0/0f/DoD_C4ISR_Framework.jpg



Raytheon

Holistic Approach to Program Protection

NDIA System Security Engineering Committee
A Path Towards Cyber Resilient and Secure Systems, April 2016

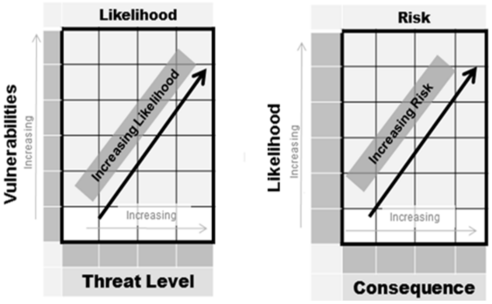
- A holistic approach to system security engineering (SSE) makes use of scientific and engineering principles to deliver assured system-level protection via a single, full-system/full life cycle view of system security. Implemented via the program protection process, SSE can enable managing and balancing risks across the security specialties such as Information Assurance/Cybersecurity, anti-tamper (AT), supply chain, software and hardware assurance, and general program security to provide a system security risk perspective.
- Taking a holistic approach to system security and bringing together multiple communities with rich histories introduces varying perspectives, terminologies, and taxonomies along with methodologies for evaluating the security quality system attributes of metrics and measures.
- System Security Challenge
  - – Contracts are awarded on technical merit, past performance, and cost.
  - – If security relevant requirements are not crisply defined with metrics and measures, system security quality attributes will be traded away to system technical capability and a more affordable solution.
  - – Today progress is being made as the presence of security relevant requirements in contract statement of work language is increasing and maturing.
  - – However, system security and program protection have not yet made it into the contract award evaluation criteria.

Raytheon

Common Metric, System Security Risk

- Each security specialty addresses a unique aspect or set of threats and vulnerabilities, and each security specialty has a unique set of countermeasures or risk mitigations.
- A common metric is needed to communicate across security specialties to minimize the security gaps and seams.
- A common metric across all the security specialties is RISK.

In general terms, risk is calculated as follows:



Raytheon

Common Risk Scale

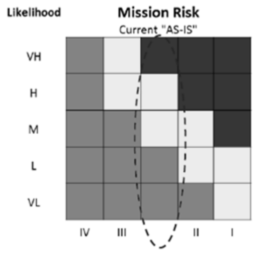
In order to communicate across security specialties, a common understanding of system security risk is needed as well as a common scale.

Each security specialty risk contributes to the composite system security risk.

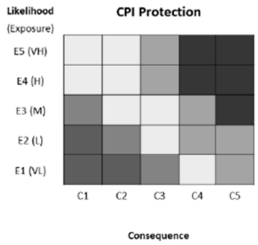
Current guidance with variation in evaluating security specialty risk and variation in the risk scales used contribute to the challenge.

In the example below, Risk ranges vary from 1-3 to 1-5.

DAG Ch13 Program Protection
Risk Assessment Guidance



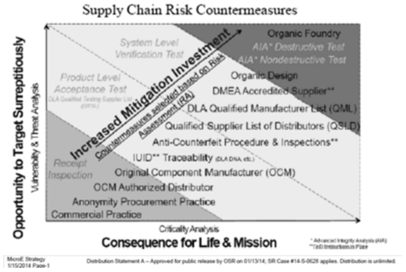
Critical Program Information (CPI)
Protection Guidance



System Security Risk or Level of Rigor Required

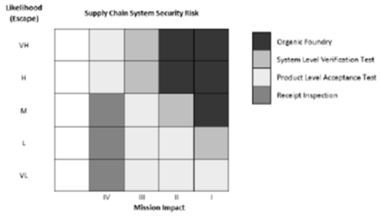
Raytheon

- Once a common metric and scale is established, levels of system security specialty risk mitigations or countermeasures can be developed that commensurate with the level of risk.
- If the countermeasures are not implemented, than the resultant risk contributes to the composite system security risk.
- CPI community already use this type of methodology. The resultant of Exposure x Consequence = Level of Protection Required.
- This methodology may also work nicely with supply chain to ensure the authenticity and integrity of components.
- The following leverages from existing guidance and offers a notional future state for supply chain.


Supply Chain Risk Countermeasures
Opportunity to Target Surreptitiously
Vulnerability & Threat Analysis
Consequence for Life & Mission
Criticality Analysis
Increased Mitigation Investment
Countermeasures selected based on Risk Assessment (RA)
System Level Verification Test
Product Level Acceptance Test
DLA Qualified Testing Supplier List (QTSL)
Receipt Inspection
Organic Foundry
AIA* Destructive Test
AIA* Nondestructive Test
Organic Design
DMEA Accredited Supplier**
DLA Qualified Manufacturer List (QML)
Qualified Supplier List of Distributors (QSLD)
Anti-Counterfeit Procedure & Inspections**
IUID** Traceability (DLA DNA, etc.)
Original Component Manufacturer (OCM)
OCM Authorized Distributor
Anonymity Procurement Practice
Commercial Practice
* Advanced Integrity Analysis (AIA)
**DoD Instructions in Place

MicroE Strategy
1/15/2014 Page-1

Distribution Statement A – Approved for public release by OSR on 01/13/14; SR Case #14-S-0628 applies. Distribution is unlimited.



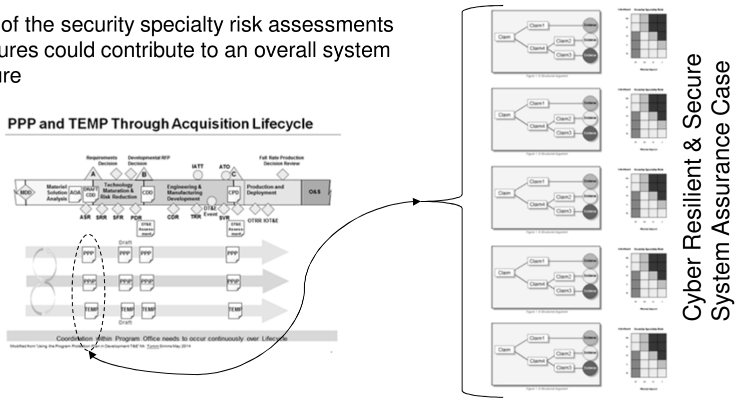
How Do We Prove System Security?

Raytheon

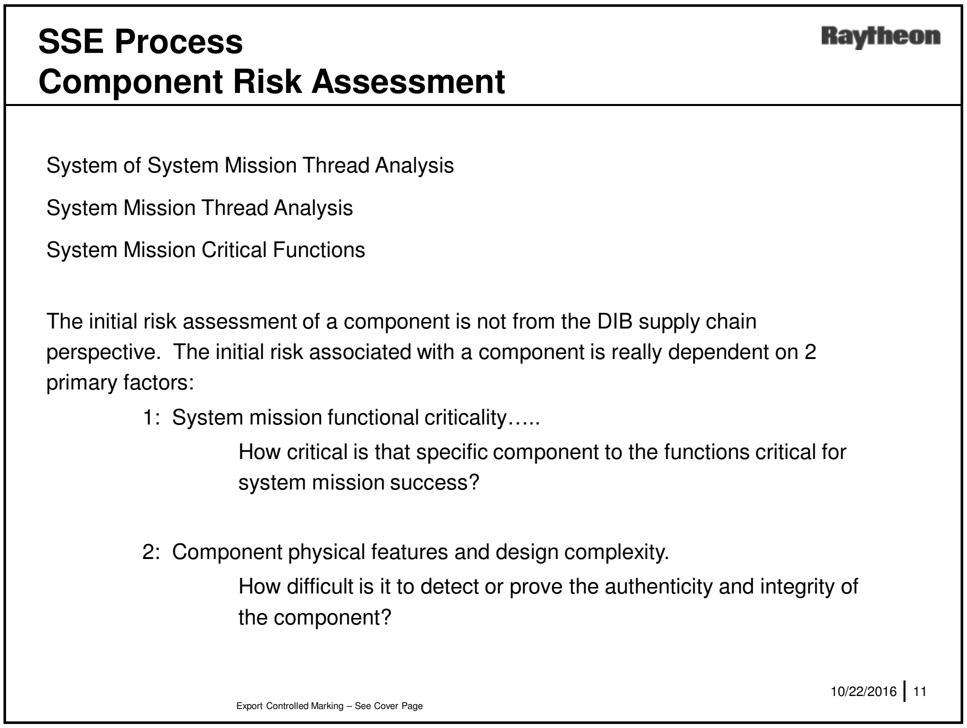
Assurance case models provide structured reasoning that engineers use implicitly to gain confidence that systems will work as expected

Evidence may include a culmination of tools, techniques, technologies, processes, and expertise.

Evidence of each of the security specialty risk assessments and countermeasures could contribute to an overall system security risk posture


PPP and TEMP Through Acquisition Lifecycle
Requirements Decision
Developmental RFP Decision
IATT
ATO
Full Rate Production Decision Review
A
B
C
MDD
Materiel Solution Analysis
AOA
DRAFT CDD
Technology Maturation & Risk Reduction
CDD
Engineering & Manufacturing Development
CPD
Production and Deployment
O&S
ASR
SRR
SFR
PDR
CDR
TRR
OT&E Event
SVR
OTRR
IOT&E
OT&E Assessment
Draft
PPP
TEMP
Coordination within Program Office needs to occur continuously over Lifecycle
Modified from "Using the Program Protection Plan in Development T&E" Mr. Tomm Simms May 2014
Claim
Claim1
Claim2
Claim3
Claim4
Cyber Resilient & Secure System Assurance Case

Cyber Resilient & Secure System Assurance Case Matures over the Lifecycle



SSE Process
Component Risk Assessment

Raytheon

System of System Mission Thread Analysis

System Mission Thread Analysis

System Mission Critical Functions

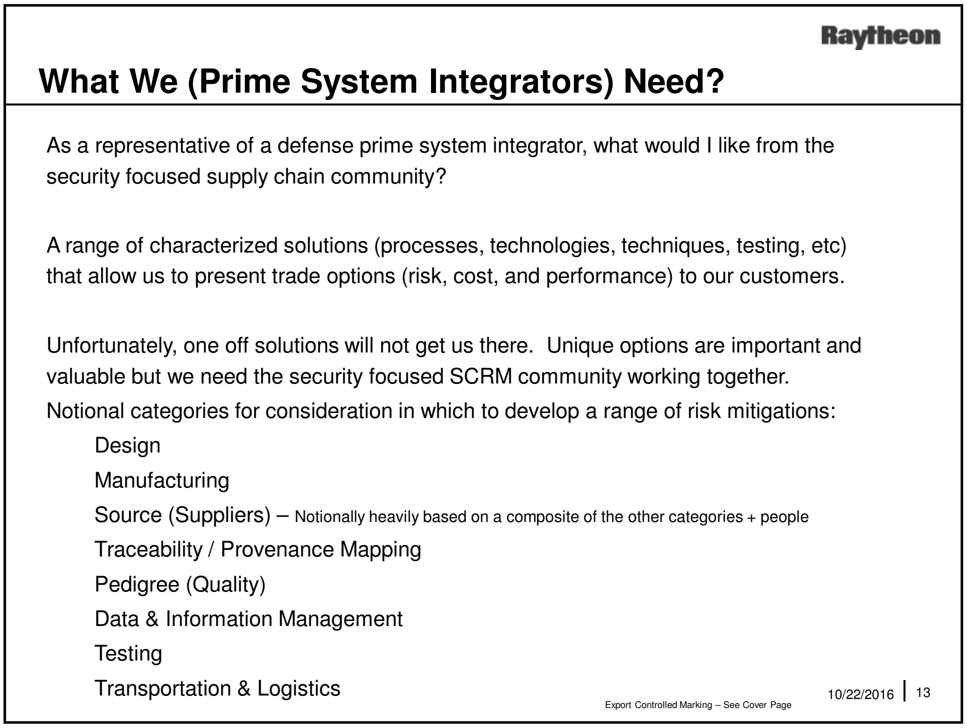
The initial risk assessment of a component is not from the DIB supply chain perspective. The initial risk associated with a component is really dependent on 2 primary factors:

1: System mission functional criticality…..

How critical is that specific component to the functions critical for system mission success?

2: Component physical features and design complexity.

How difficult is it to detect or prove the authenticity and integrity of the component?



Raytheon

What We (Prime System Integrators) Need?

As a representative of a defense prime system integrator, what would I like from the security focused supply chain community?

A range of characterized solutions (processes, technologies, techniques, testing, etc) that allow us to present trade options (risk, cost, and performance) to our customers.

Unfortunately, one off solutions will not get us there. Unique options are important and valuable but we need the security focused SCRM community working together.

Notional categories for consideration in which to develop a range of risk mitigations:

Design

Manufacturing

Source (Suppliers) – Notionally heavily based on a composite of the other categories + people

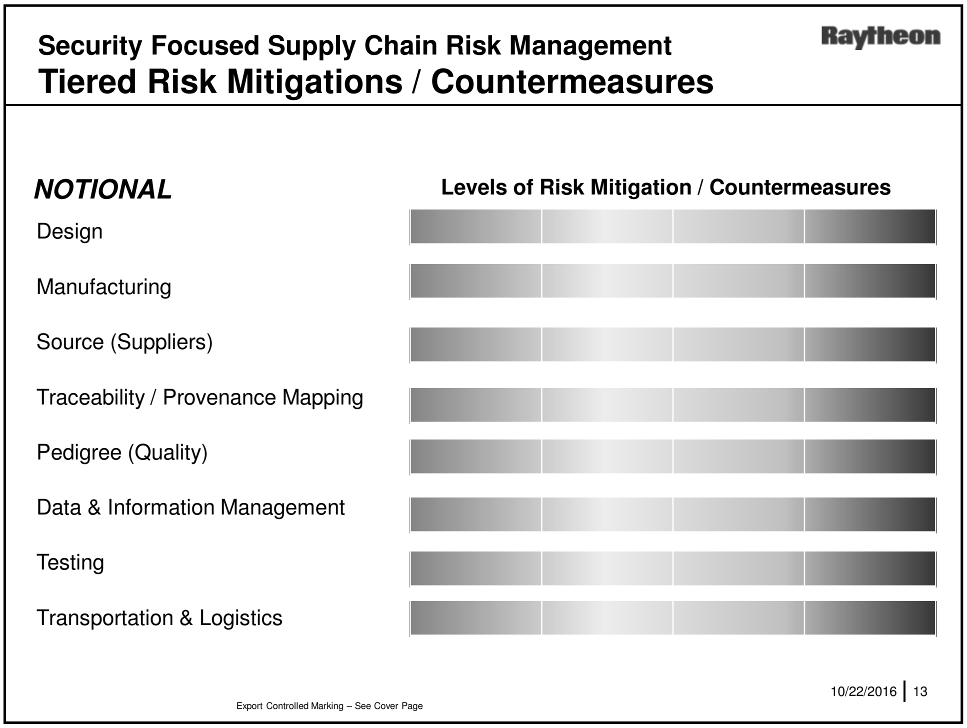
Traceability / Provenance Mapping

Pedigree (Quality)

Data & Information Management

Testing

Transportation & Logistics



Security Focused Supply Chain Risk Management

Tiered Risk Mitigations / Countermeasures

Raytheon

NOTIONAL

Levels of Risk Mitigation / Countermeasures

Design

Manufacturing

Source (Suppliers)

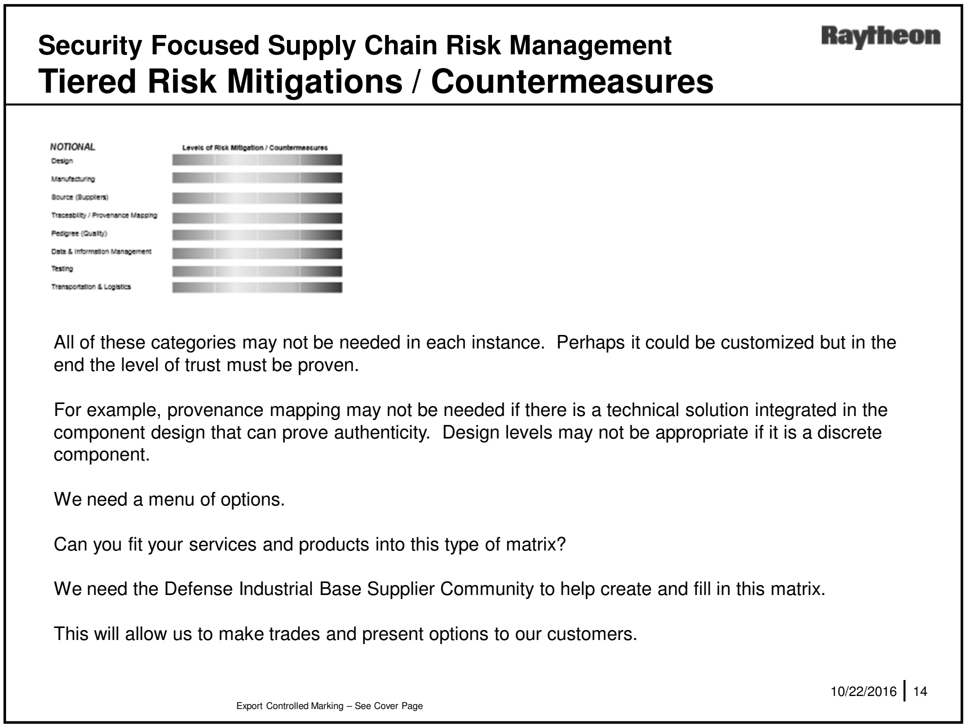
Traceability / Provenance Mapping

Pedigree (Quality)

Data & Information Management

Testing

Transportation & Logistics



Security Focused Supply Chain Risk Management

Tiered Risk Mitigations / Countermeasures

Raytheon

NOTIONAL
Levels of Risk Mitigation / Countermeasures
Design
Manufacturing
Source (Suppliers)
Traceability / Provenance Mapping
Pedigree (Quality)
Data & Information Management
Testing
Transportation & Logistics

All of these categories may not be needed in each instance. Perhaps it could be customized but in the end the level of trust must be proven.

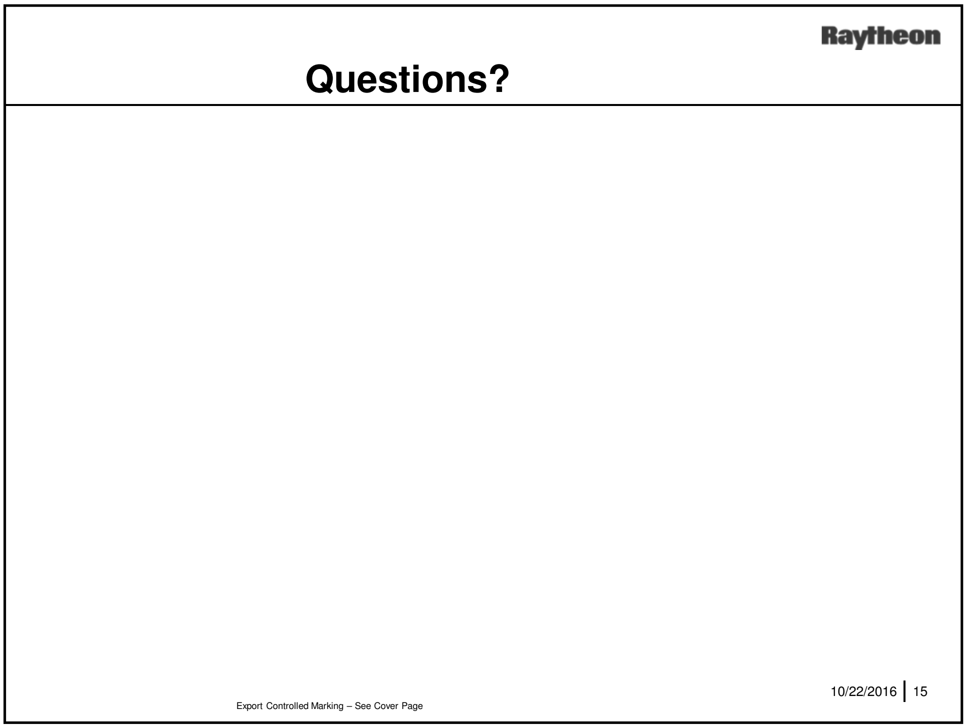
For example, provenance mapping may not be needed if there is a technical solution integrated in the component design that can prove authenticity. Design levels may not be appropriate if it is a discrete component.

We need a menu of options.

Can you fit your services and products into this type of matrix?

We need the Defense Industrial Base Supplier Community to help create and fill in this matrix.

This will allow us to make trades and present options to our customers.



Raytheon

Questions?

Export Controlled Marking – See Cover Page

10/22/2016 | 15