SAND2017-6389C

2017 Contractors Internal Audit Directors (CIAD) Conference

TRUST in the Supply Chain

Presenter: Delfinia Salazar, Manager, Supply Chain Risk Management
Sandia National Laboratories

NREL NATIONAL RENEWABLE ENERGY LABORATORY

DOE Contractors CIAD Internal Audit Directors

washington river protection solutions

Learning Objectives

- At the completion of this program, the participants will be able:
  - To describe TRUST and Supply Chain Risk Management
  - To question red flags throughout the supply chain
  - To contrast a TRUST risk assessment to a general risk assessment

Supply Chain Risk Management and TRUST

Intelligence.Gov Background Paper

- *Per the National Counterintelligence and Security Center Supply Chain Directorate (NCSC), Office of the Director of National Intelligence, Background Paper: insight into SCRM concepts and NCSC's mission*
  - A major factor enabling supply chain threats has been the **globalization** of our supply chains, characterized by a **complex web of contracts** and subcontracts for component parts, services, and manufacturing extending across the country and around the world.
  - The multiple layers and networks of suppliers in this chain are frequently not well understood by either manufacturers or consumers.
  - Our most capable **adversaries** can **access this supply chain** at multiple points, establishing advanced, persistent, and multifaceted subversion.
  - Our adversaries are also able to use this complexity to **obfuscate** their efforts to **penetrate** sensitive research and development programs, **steal** intellectual property (IP) and personally identifiable information (PII), **insert** malware into critical components, and **mask** foreign ownership, control, and/or influence (FOCI) of key providers of components and services.
  - **Individually and in total, these supply chain attacks erode our nation's competitive advantages in commerce, technology, and security.**

What is Supply Chain Risk Management (SCRM)?

- *As defined by the Office of the Director of National Intelligence (ODNI) Intelligence Community Directive (ICD)-731*
  - SCRM is the management of risk to the integrity, trustworthiness, and authenticity of products and services within the supply chain.
  - It addresses the activities of foreign intelligence entities and any other adversarial attempts aimed at compromising the supply chain, which may include the introduction of counterfeit or malicious items into the supply chain."

DOE/NNSA Requirements That Support a Robust SCRM Program

Prime Contract Requirements to identify, assess, evaluate, and mitigate supply chain, acquisition, and supplier risks in Nuclear Enterprise Assurance (NEA), cyber, intelligence, quality, and others.

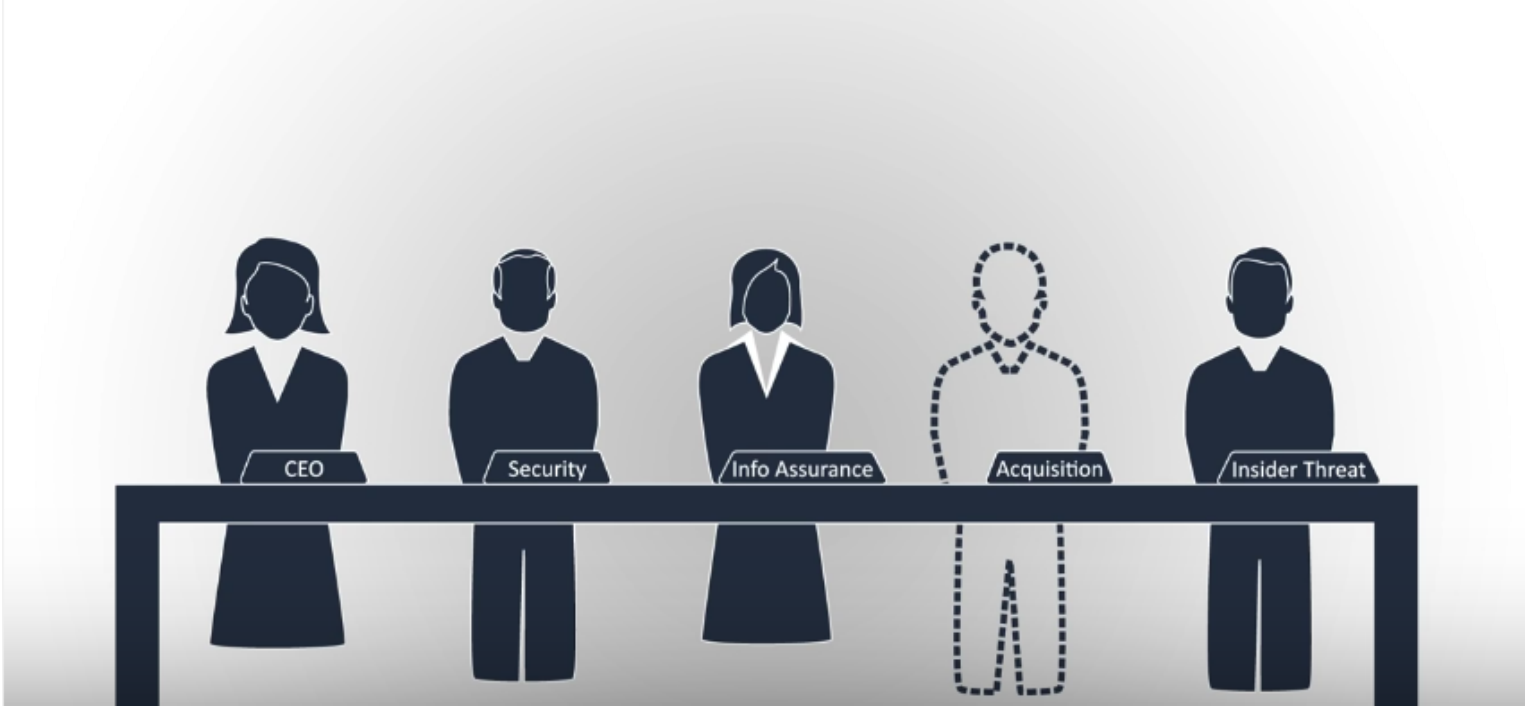
Select requirements include:

- **NAP-24A, *NNSA Weapons Quality Policy***
- DOE O 414.1D, *Quality Assurance*
- NAP 14.1-D, *Baseline Cyber Security Program*
- DOE O 205.1B, *Department of Energy Cyber Security Program*
- DOE O 471.6, *Information Security*
- Related to EO 12333, ODNI ICD 731, *Supply Chain Risk Management*

TRUST – As Embodied in DOE/NNSA Policy (NAP-24A, Attachment 4)

Select content removed for UUR distribution

Video: “Know the Risk - Raise Your Shield: Supply Chain Risk Management”



Published on Aug 11, 2016
Prepared by the Office of the Director of National Intelligence's National Counterintelligence and Security Center

Supply Chain Cycle – Considers Risks and Red Flags

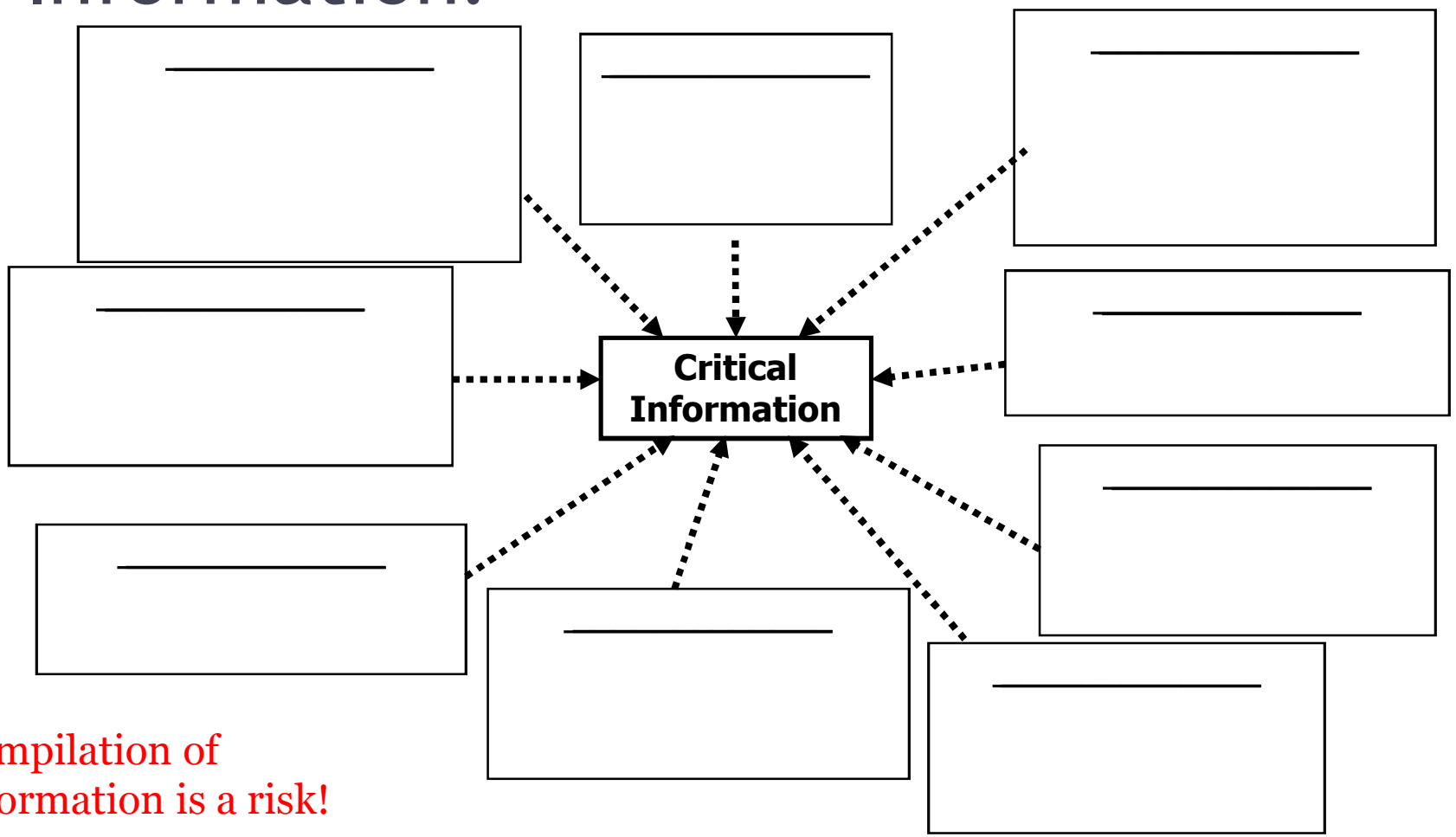
Supply Chain Cycle – Where Are the Risks?

Example:

Risk: Suspect parts are received

Control & Response: Detect, Report, and Mitigate Suspect/ Counterfeit parts

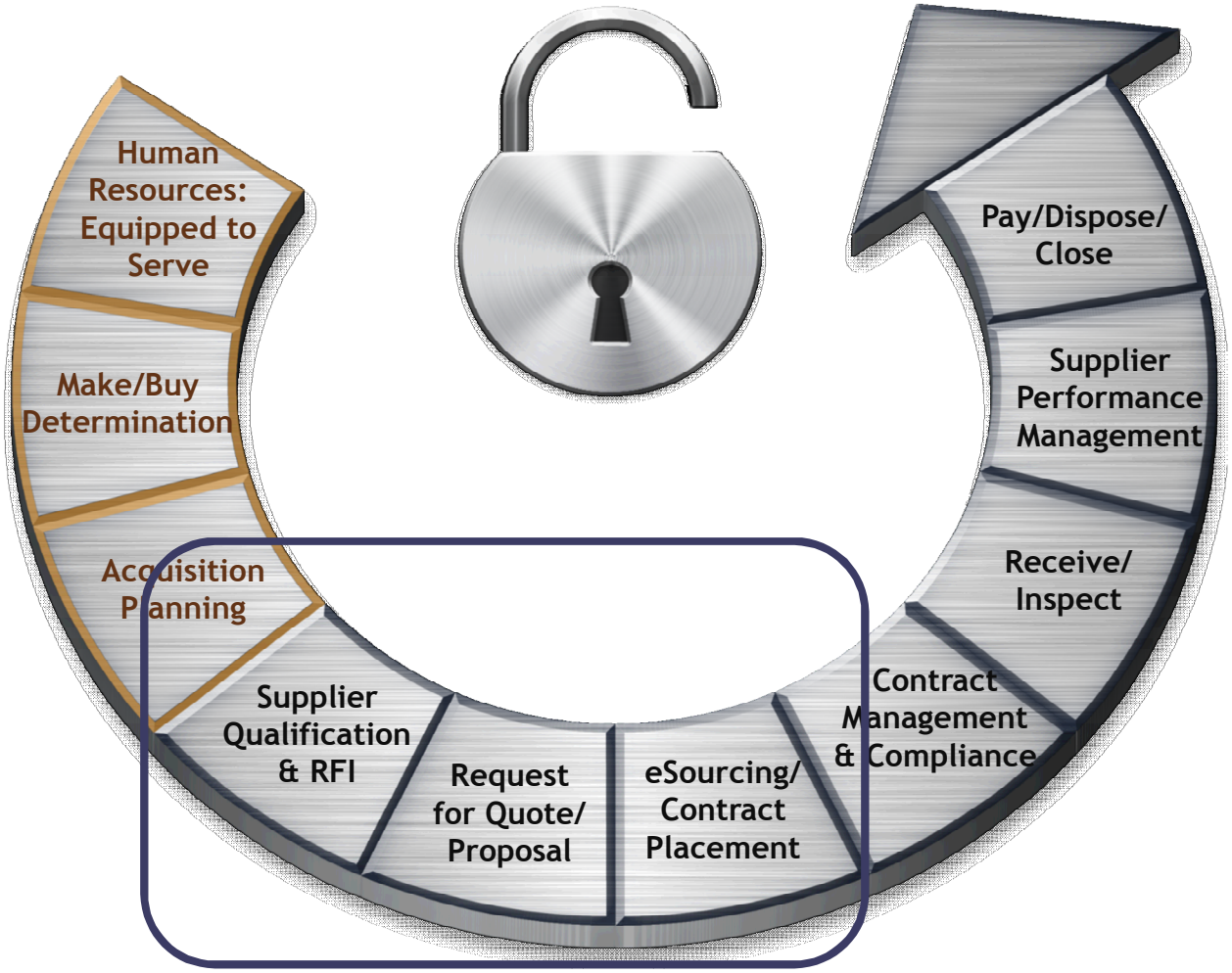
What may be Critical Supply Chain Information?



Compilation of information is a risk!

Select content removed for UUR distribution

Supply Chain Cycle – What are Possible Red Flags?

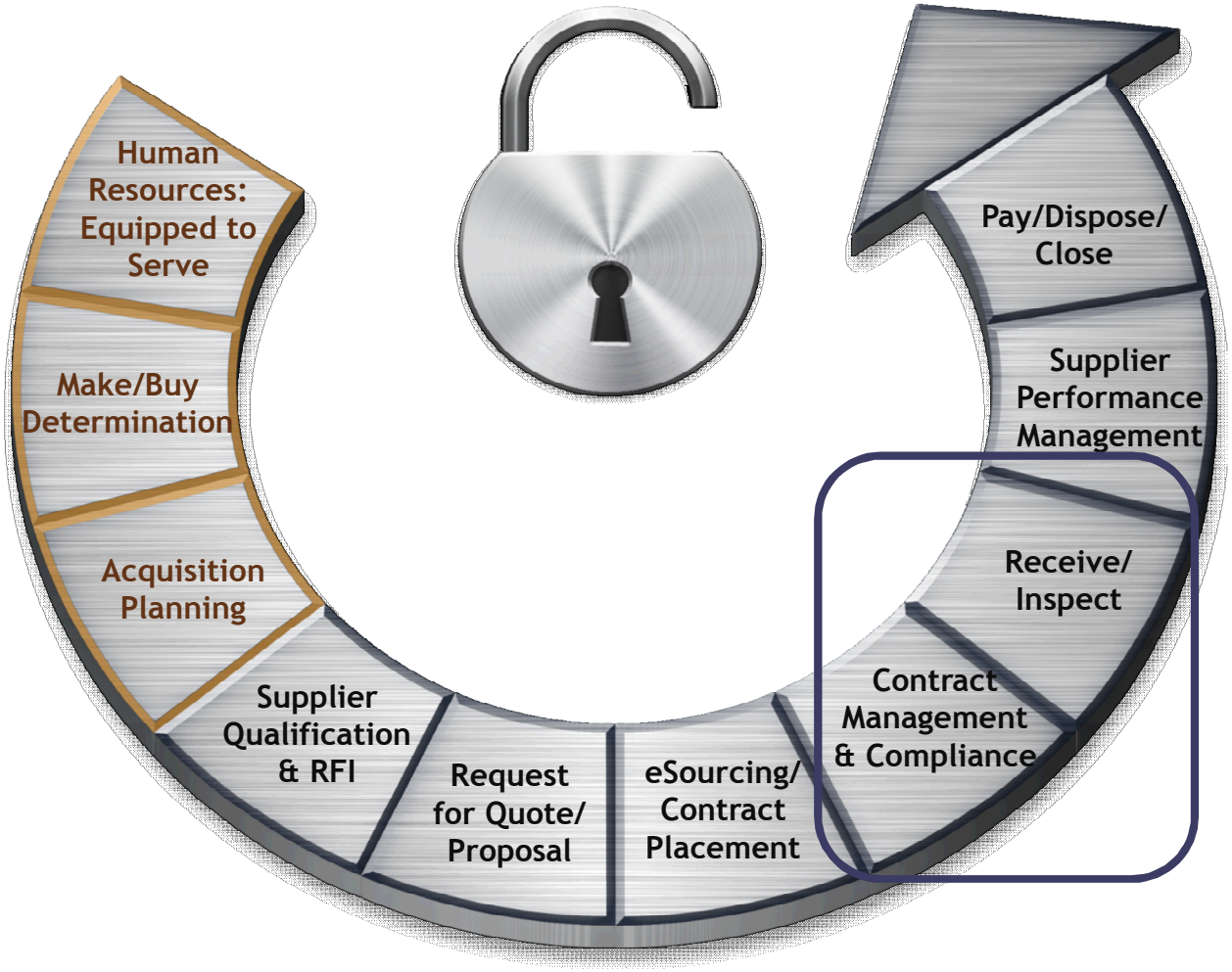


Source: SCRM training at SNL and KCNSC

Sourcing/Negotiation – Red Flags

Select content removed for UUR distribution

Supply Chain Cycle – What are Possible Red Flags?



Source: SCRM training at SNL and KCNSC

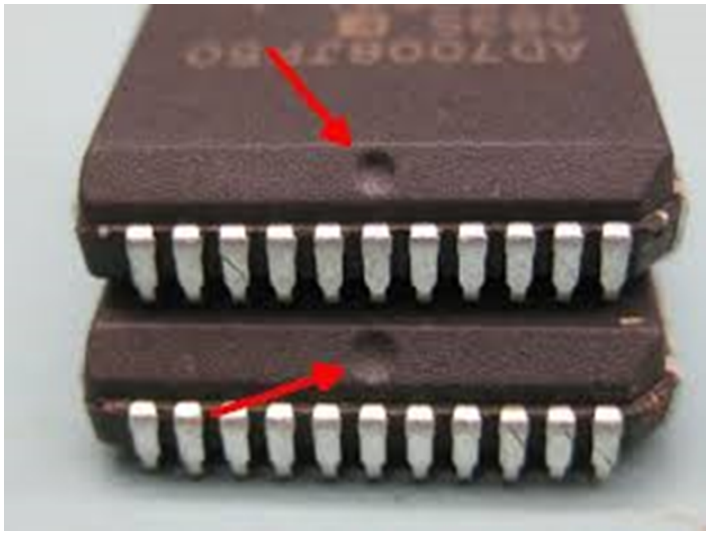
Manage Contract & Receive Items – Red Flags

Select content removed for UUR distribution

What are Suspect or Counterfeit Items?

- **Suspect** Item- May have been misrepresented (looks weird, but no definitive proof of fraud, misrepresentation, Intellectual Property infringement, etc.)

These are the same part but look different.
This is considered "Suspect".



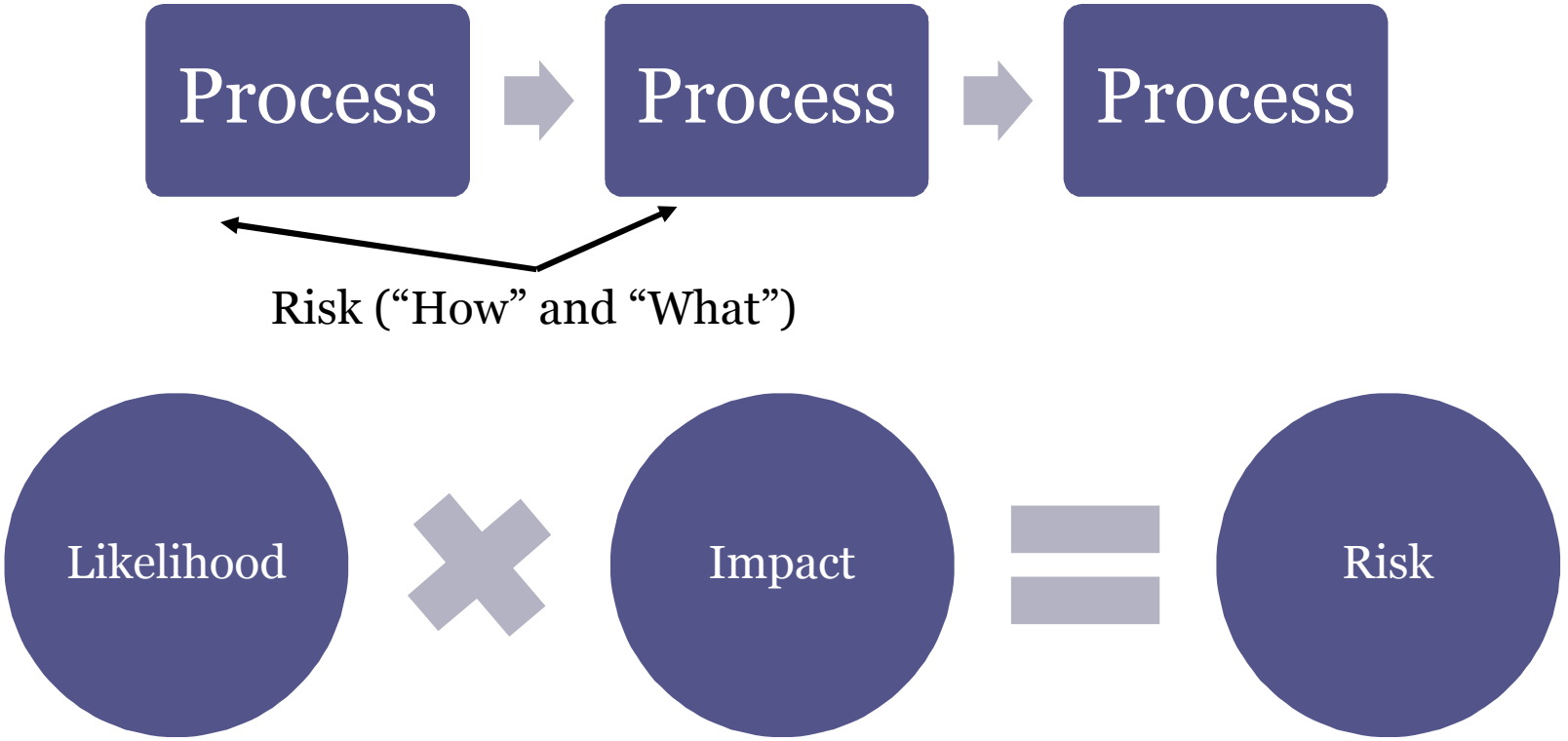
What are Suspect or Counterfeit Items?

- **Counterfeit-** Definitive proof of misrepresentation, fraud, or Intellectual Property infringement

This item was painted "blacktopped" and remarked with a different manufacturer and part number. This would be considered "Counterfeit."

Evolving to a TRUST Risk Assessment

Common Risk Assessment



TRUST Risk Assessment Process

Additional TRUST Layer

Common Risk Assessment Approach

Vulnerability Assessment

- Proposed Acquisition – when, where, how is it vulnerable?

Impact Assessment

- Potential adverse impacts or potential harm
- Likelihood and impact

Risk

Select content removed for UUR distribution

Lessons from 2017 SCRM Workshop

- 3rd Annual Supply Chain Risk Management/ Weapons TRUST Assurance Workshop
- Participants:

- Notable lessons:

Select content removed for UUR distribution

Consider: Key Players in a TRUST Risk Assessment

- Program Staff
- Counterintelligence
- Acquisitions / Supply Chain
- Security
- Information Assurance / Information Technology
- Risk Officers
- Others?

Summary

Summary

- To secure the supply chain, the entire supply chain process needs to be understood.
- TRUST risk assessments add the element of _____.
- A well-rounded team should be considered when identifying and analyzing supply chain _____, _____, and _____.

Questions