Adding a Security Assurance Dimension to Supply Chain Practices

John Whited, CISSP, CSSLP

Randall Brooks, CISSP, CSSLP

Raytheon Company

Session ID: GRC-401

Session Classification: Intermediate

RSA CONFERENCE 2012

Agenda

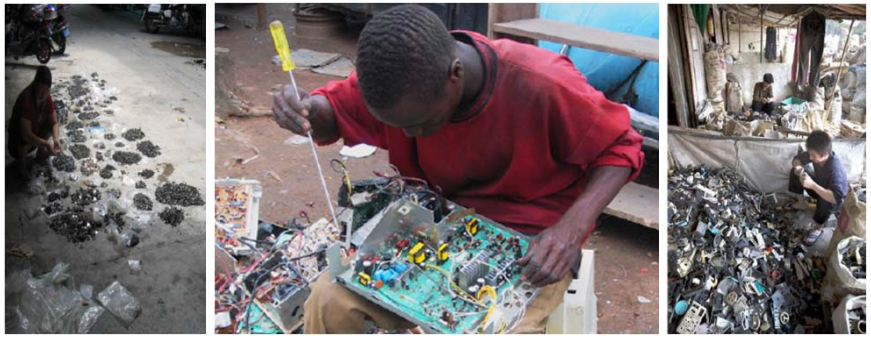
- What is the Supply Chain Problem?
- Legacy Supply Chain Practices
  - Acquisition
  - Subcontract management
- Best Practices
  - Industry
  - Government
  - Academia
- An Approach for Cyber Supply Chain Assurance
- Key Takeaways
- Q&A

What is the Supply Chain Problem?
Key Takeaways

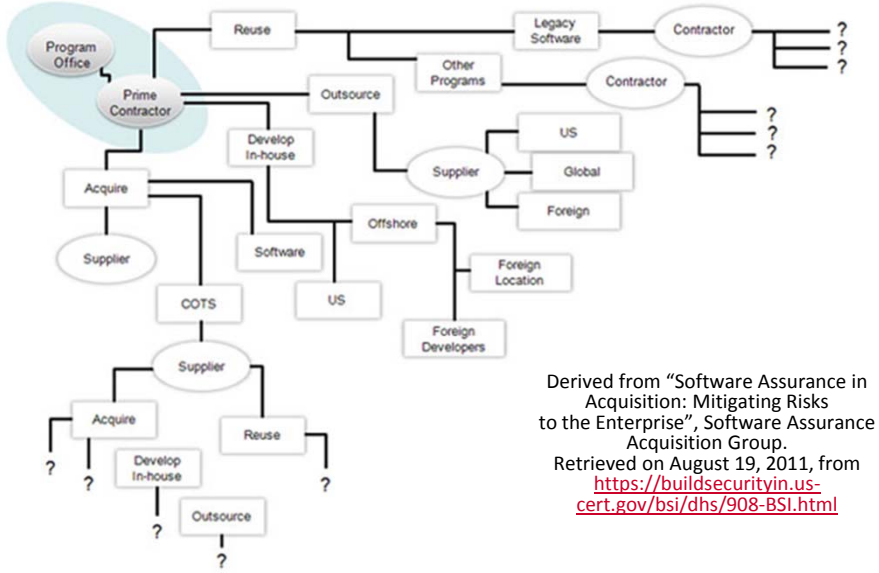
- Vulnerabilities exist within one's supply chain
- A system's risk has many factors
- Systems and Software Assurance (SSwA) evaluation of both supplier and product may be required
- SSwA should be in all 3rd party contracts
- Observe the next level supplier principle

What is the Supply Chain Problem?
From the Headlines

- Most counterfeit parts are intentionally put into the supply chain to make a profit… However…
- Malicious actors also embed malware
  - "The Navy Bought Fake Chinese Microchips That Could Have Disarmed U.S. Missiles"
  - Excerpts
    - Last year, the U.S. Navy bought 59,000 microchips were counterfeits
    - Could have rendered missiles useless



Global Supply Chain

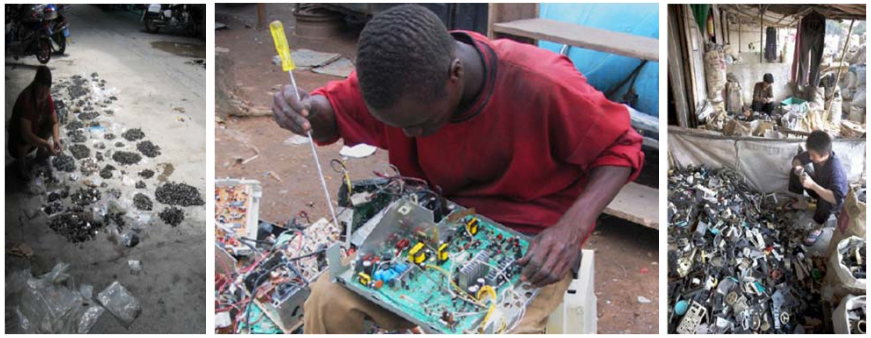


Derived from "Software Assurance in Acquisition: Mitigating Risks to the Enterprise", Software Assurance Acquisition Group. Retrieved on August 19, 2011, from https://buildsecurityin.us-cert.gov/bsi/dhs/908-BSI.html

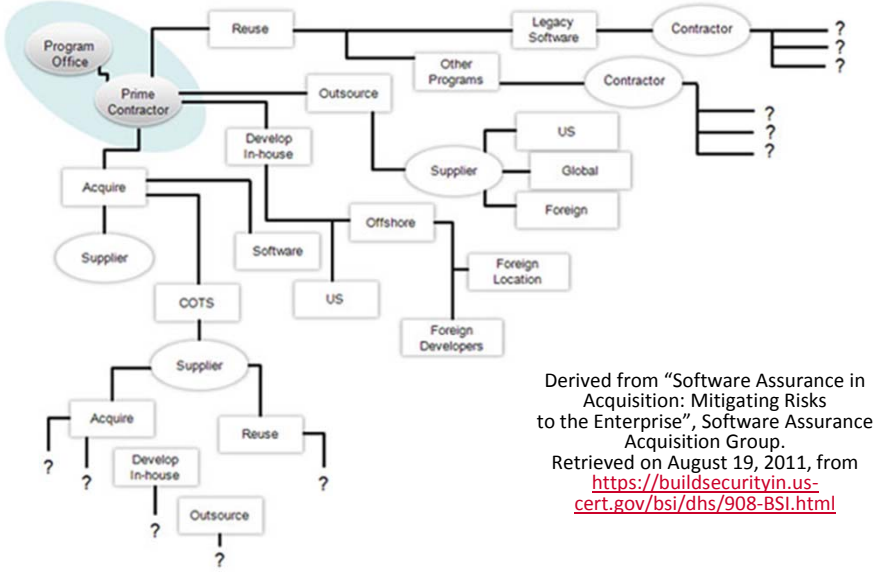
http://articles.businessinsider.com/2011-06-27/news/30048253_1_microchips-missiles-foreign-chip-makers

What is the Supply Chain Problem?
From the Headlines

- Most counterfeit parts are intentionally put into the supply chain to make a profit… However…
- Malicious actors also embed malware
  - "The Navy Bought Fake Chinese Microchips That Could Have Disarmed U.S. Missiles"
  - Excerpts
    - Last year, the U.S. Navy bought 59,000 microchips were counterfeits
    - Could have rendered missiles useless



Global Supply Chain



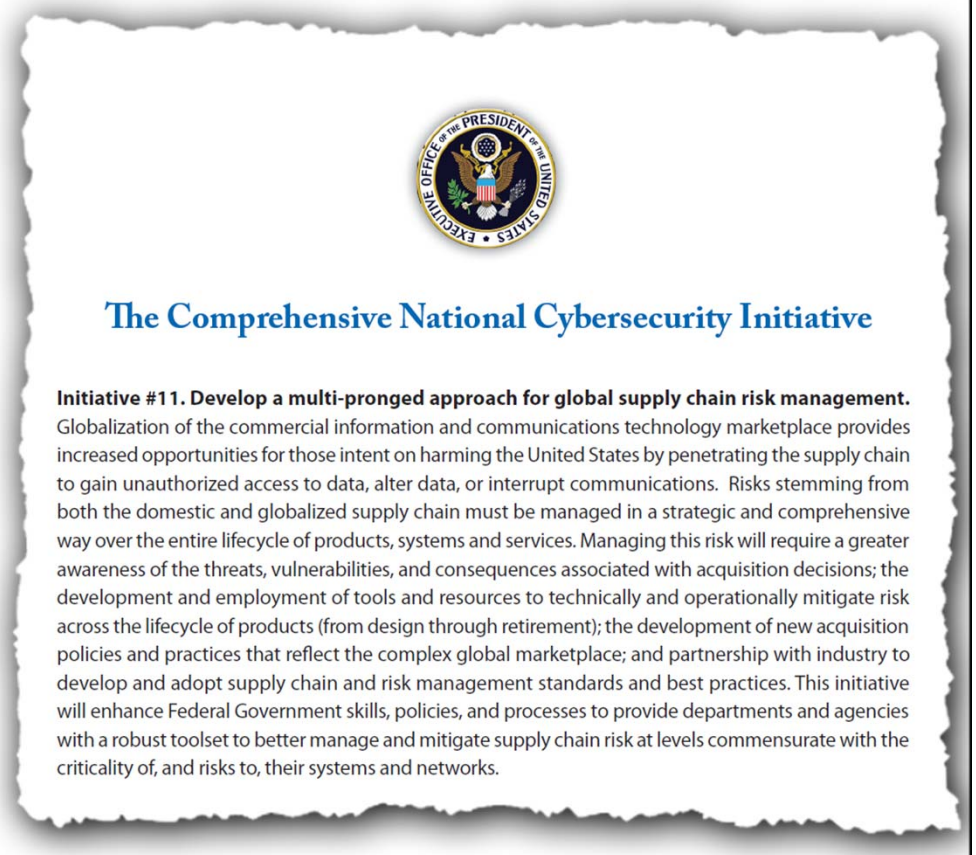
Derived from "Software Assurance in Acquisition: Mitigating Risks to the Enterprise", Software Assurance Acquisition Group. Retrieved on August 19, 2011, from https://buildsecurityin.us-cert.gov/bsi/dhs/908-BSI.html

http://articles.businessinsider.com/2011-06-27/news/30048253_1_microchips-missiles-foreign-chip-makers

What is the Supply Chain Problem?

US Govt. recognition: Comprehensive National Cybersecurity Initiative (CNCI)

- CNCI – White House initiatives to help secure the United States in cyberspace
- Initiative 11
  - An approach for global cyber supply chain risk management
  - Focused on a robust toolset to better manage and mitigate supply chain risk



The Comprehensive National Cybersecurity Initiative

Initiative #11. Develop a multi-pronged approach for global supply chain risk management. Globalization of the commercial information and communications technology marketplace provides increased opportunities for those intent on harming the United States by penetrating the supply chain to gain unauthorized access to data, alter data, or interrupt communications. Risks stemming from both the domestic and globalized supply chain must be managed in a strategic and comprehensive way over the entire lifecycle of products, systems and services. Managing this risk will require a greater awareness of the threats, vulnerabilities, and consequences associated with acquisition decisions; the development and employment of tools and resources to technically and operationally mitigate risk across the lifecycle of products (from design through retirement); the development of new acquisition policies and practices that reflect the complex global marketplace; and partnership with industry to develop and adopt supply chain and risk management standards and best practices. This initiative will enhance Federal Government skills, policies, and processes to provide departments and agencies with a robust toolset to better manage and mitigate supply chain risk at levels commensurate with the criticality of, and risks to, their systems and networks.

What is the Supply Chain Problem?

US Govt. recognition:
Ike Skelton 2011 National Defense Authorization Act (NDAA)

- NDAA Section 806:
  Requirements for Information Relating to Supply Chain Risk:
  - The exclusion of a source that fails to meet qualification standards estab… n 2319 of title 1… upply chain risk in the acquisition of covered systems *
  - The exclusion of a source that fails to achieve an acceptable rating with … leration of supp… ard of a contract or the issuance of a task or delivery order
  - The decision to withhold consent for a contractor to subcontract with … ntract with a particular source or to direct a contractor syste… red for a subcontract under the contract.

* **COVERED SYSTEM** – The term "covered system" means a national security system, as that term is defined in section 3542(b) of title 44, United States Code.

What is the Supply Chain Problem?

US Govt. recognition:
Ike Skelton 2011 National Defense Authorization Act (NDAA)

- Other Gotcha's

Supplier can be banned… without notification…
Without ability to appeal decision…
Other DoD agencies will be notified!

Legacy Supply Chain Practices
Acquisition

- Common Acquisition Questions about Vendors:
  - Preferred vendor list?
  - Banned vendor list?
  - Foreign country?
  - Financially stable?
  - Prior experience?
  - On-time delivery?
  - High quality?

Legacy Supply Chain Practices
Subcontract Management

- Common Contract Points:
  - Description and quantity of product to be delivered
  - Delivery schedule
  - Payment schedule, including possible penalty for late delivery
  - Quality requirements
- All Well and Good…
  But What's Missing?
  - Product security requirements
  - Anti-counterfeit measures
  - Software assurance
  - Measurable or demonstratable evidence of vendor compliance

Best Practices (Industry)
Managing Risks Through Contracts

- A contract can only cover two levels removed:
  - The supplying entity
  - That supplier's next level of supply chain
- One must require that their suppliers ensure that each supplier's next level of supply following sound Cyber Supply Chain practices.

Best Practices (Government)
Systems and Software Assurance

"System Assurance (SA) provides the justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle."

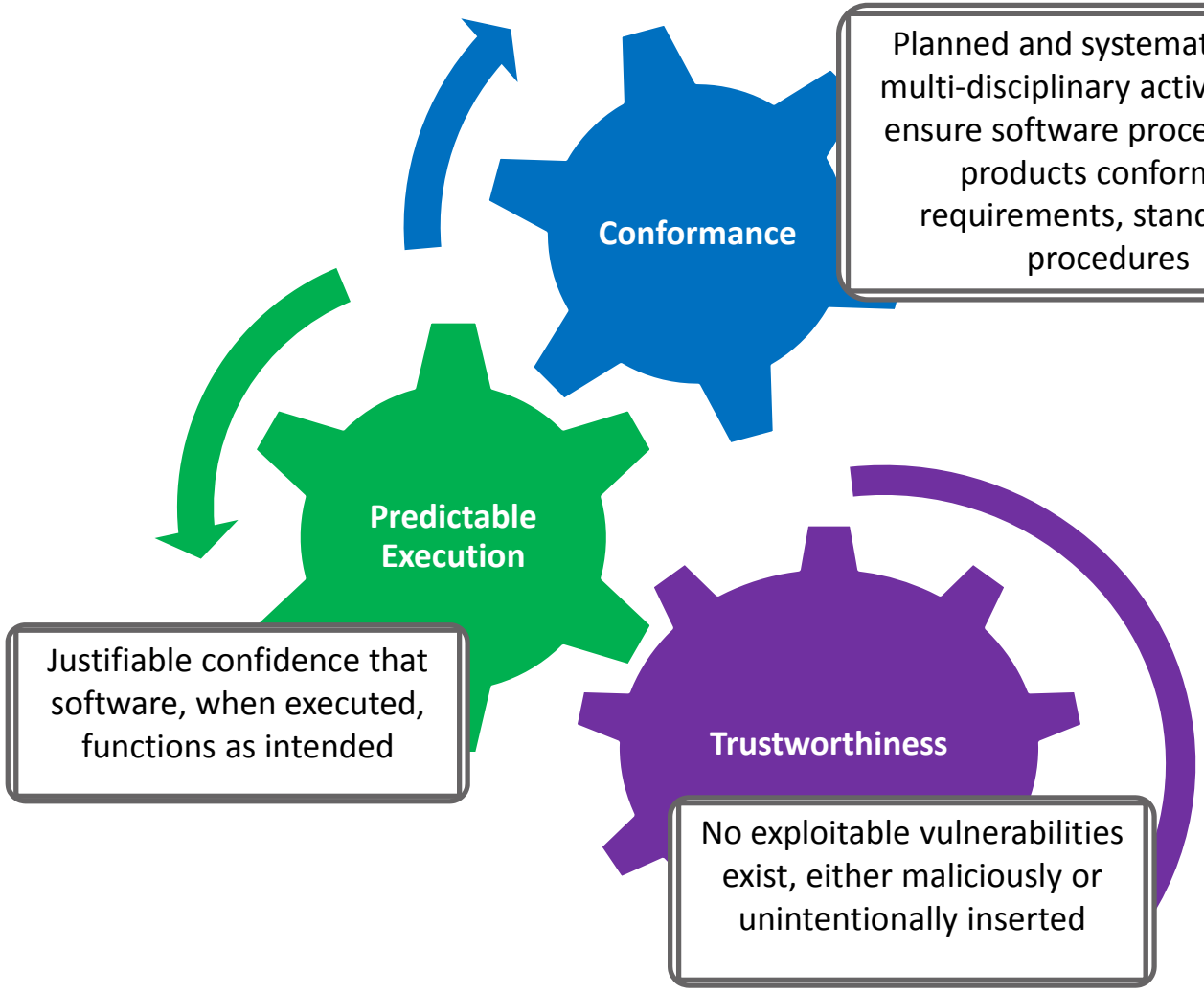
Source: National Defense Industrial Association Guidebook (Oct 2008)

Source: http://www.safecode.org/

"Software assurance is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its life cycle, and the software functions in the intended manner"

Source: CNSS Instruction No. 4009, National IA Glossary

Best Practices (Government)
SwA Addresses



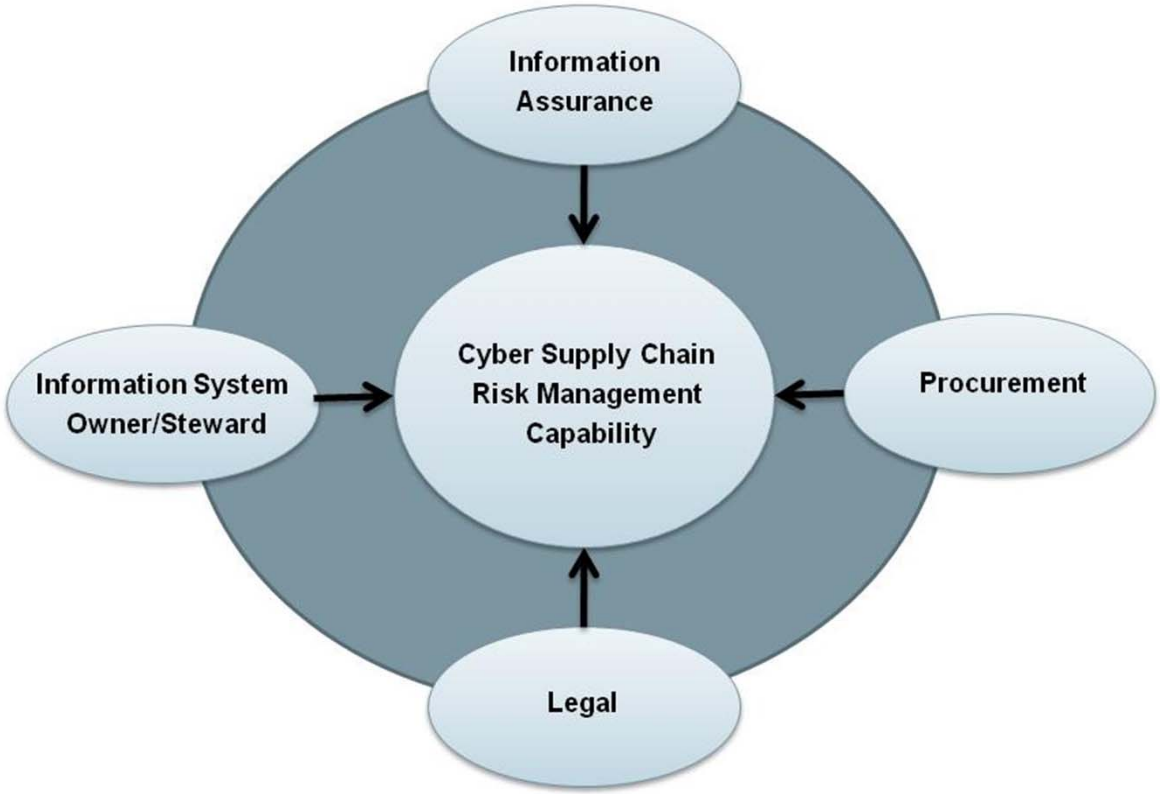
DHS Software Assurance Forum
Build Security In

https://buildsecurityin.us-cert.gov

Best Practices (Government)

NISTIR 7622 Piloting Supply Chain Risk Management for Federal Information Systems

Supply Chain Risk Management promotes integrity, security, and reliability in hardware and software code development.



Source: http://csrc.nist.gov/publications/drafts/nistir-7622/draft-nistir-7622.pdf

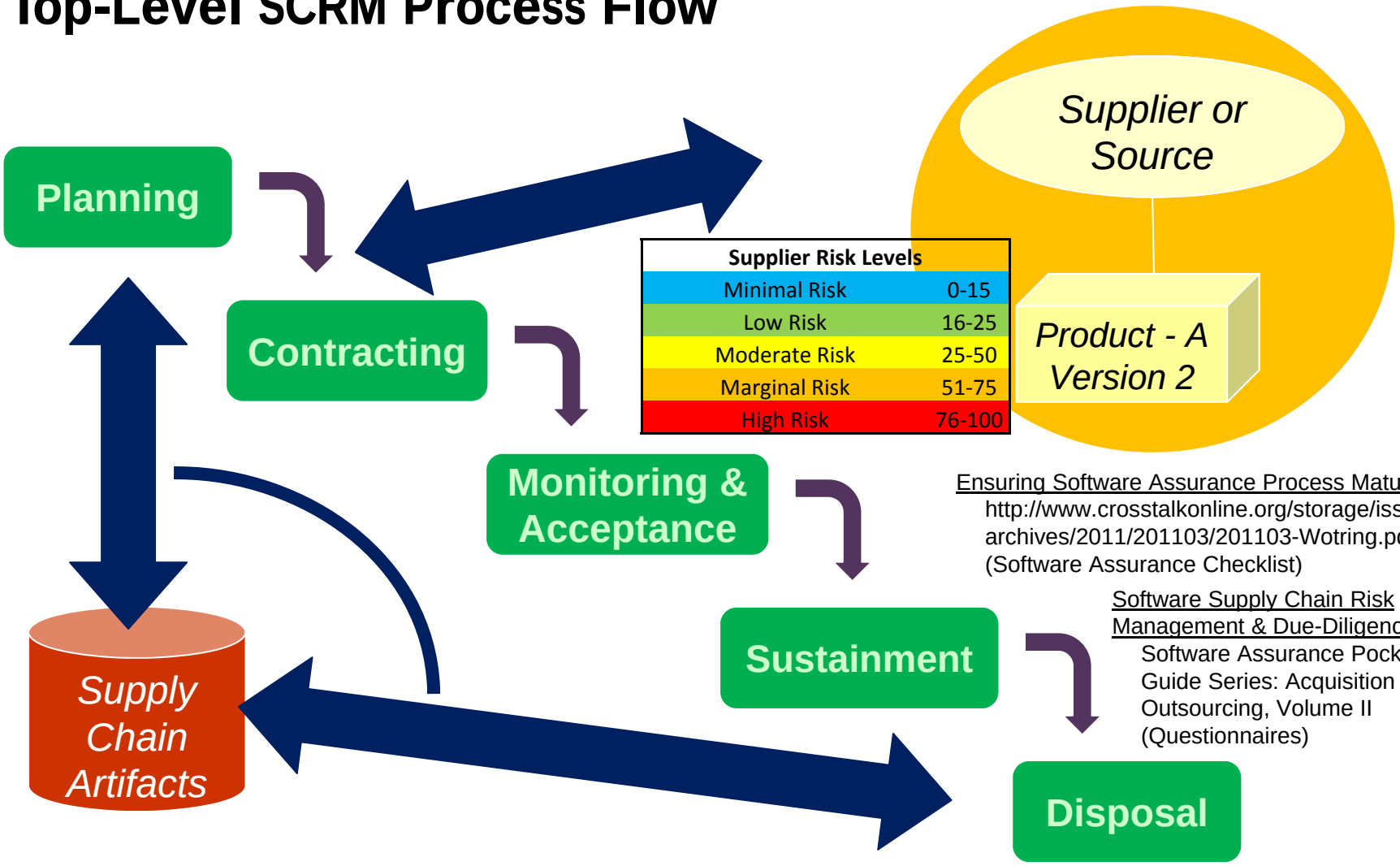
Best Practices (Government)

Controls and Guidance

- NIST 800-53
- NIST 800-37
- NIST 800-30
- NIST 800-39
- NIST 800-27
- NIST 800-64

An Approach for Cyber Supply Chain Assurance

Top-Level SCRM Process Flow



Ensuring Software Assurance Process Maturity
http://www.crosstalkonline.org/storage/issue-archives/2011/201103/201103-Wotring.pdf
(Software Assurance Checklist)

Software Supply Chain Risk Management & Due-Diligence:
Software Assurance Pocket Guide Series: Acquisition & Outsourcing, Volume II (Questionnaires)

Software Assurance in Acquisition: Mitigating Risks to the Enterprise
https://buildsecurityin.us-cert.gov/swa/downloads/SwA_in_Acquisition_102208.pdf

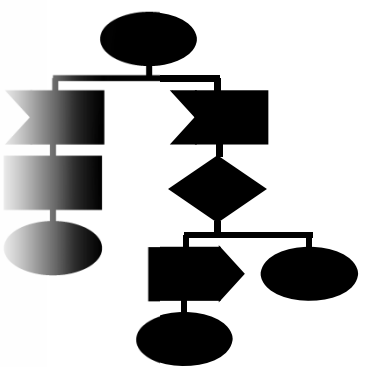
An Approach for Cyber Supply Chain Assurance
Recommendations Common to Both Software and Hardware

- Supplier business assessment
- Supplier secure development assessment
  - Supplier or source
  - Product model / version
- Acquirer business risk
- End customer mission criticality and mission assurance
- Subcontract management
  - Supplier management practices for their suppliers

An Approach for Cyber Supply Chain Assurance
Recommendations Specific to Hardware

- Quality vs. counterfeiting vs. malicious alteration
- ASICS, FPGAs, and microprocessors
- Information storage in volatile memory and permanent storage
- Nano tagging

An Approach for Cyber Supply Chain Assurance
Recommendations Specific to Software



- Recognize applicable steps to type of software
  - COTS: Source code scans not generally possible
  - Contracted software: Require 3rd party to escrow source
  - Open source and freeware, a.k.a. Free &Open Source (FOSS):
    - Cannot impose contractual terms
    - Watch for EULA and copyright issues (license management)
- Common concern for all types of software supply
  - Software pedigree: where did it come from?
    - What do I know about the original source of supply?
    - How can I authenticate the original software source of supply?
  - Software provenance: where has it been?
    - How do I know what I'm getting is what the original source produced?

Apply Slide

- How to Apply What You Have Learned Today?
  - Over the next month one should:
    - Read SwA Pocket Guides
    - Review your existing corporate supply chain practices
    - Review your existing subcontract language
    - Watch for SSwA assessment within those processes
  - Within three months you should:
    - Develop a plan to close identified gaps
  - Within six months you should:
    - Implement the plan
    - Pilot application of the plan to a candidate acquisition

What is the Supply Chain Problem?
Key Takeaways

- Vulnerabilities exist within one's supply chain
- A system's risk has many factors
- Systems and Software Assurance (SSwA) evaluation of both supplier and product may be required
- SSwA should be in all 3rd party contracts
- Observe the next level supplier principle

Questions and Answers

John Whited
john.whited@raytheon.com

Randall Brooks
brooks@raytheon.com

http://rtncyberjobs.com