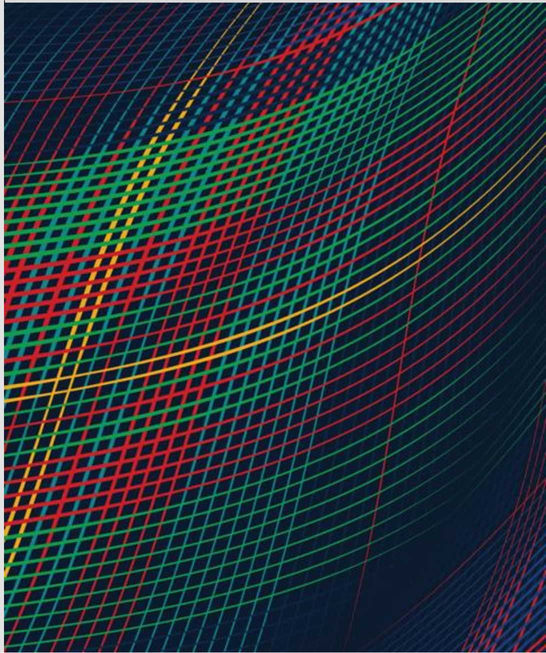
Carnegie Mellon University
Software Engineering Institute



Addressing Today’s Software Risks Requires an Assurance Educated Workforce

MARCH 19, 2025

Carol Woody, Ph.D.
Principal Researcher

Document Markings

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM25-0407

Government is Not Prepared to Adopt Commercial Approaches Successfully

Major Government Modernization Programs are attempting adoption of commercially successful approaches to improve delivery speed and reduce cost such as:

- Hardware-based solution replaced by Software-intensive system
- Waterfall methodology replaced by Agile, DevSecOps, MBSE approaches
- Program owned infrastructure replaced by Shared infrastructures (Cloud)

Potentially unintended consequences:

- Shifts in key responsibilities to different acquisition program participants without training and knowledge in how to address them
- Gaps in software understanding needed to address management and engineering change to produce software assured products
- Added complexity, interfaces, and supply chain/technology risk

DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution

“The DoD is in the software business”

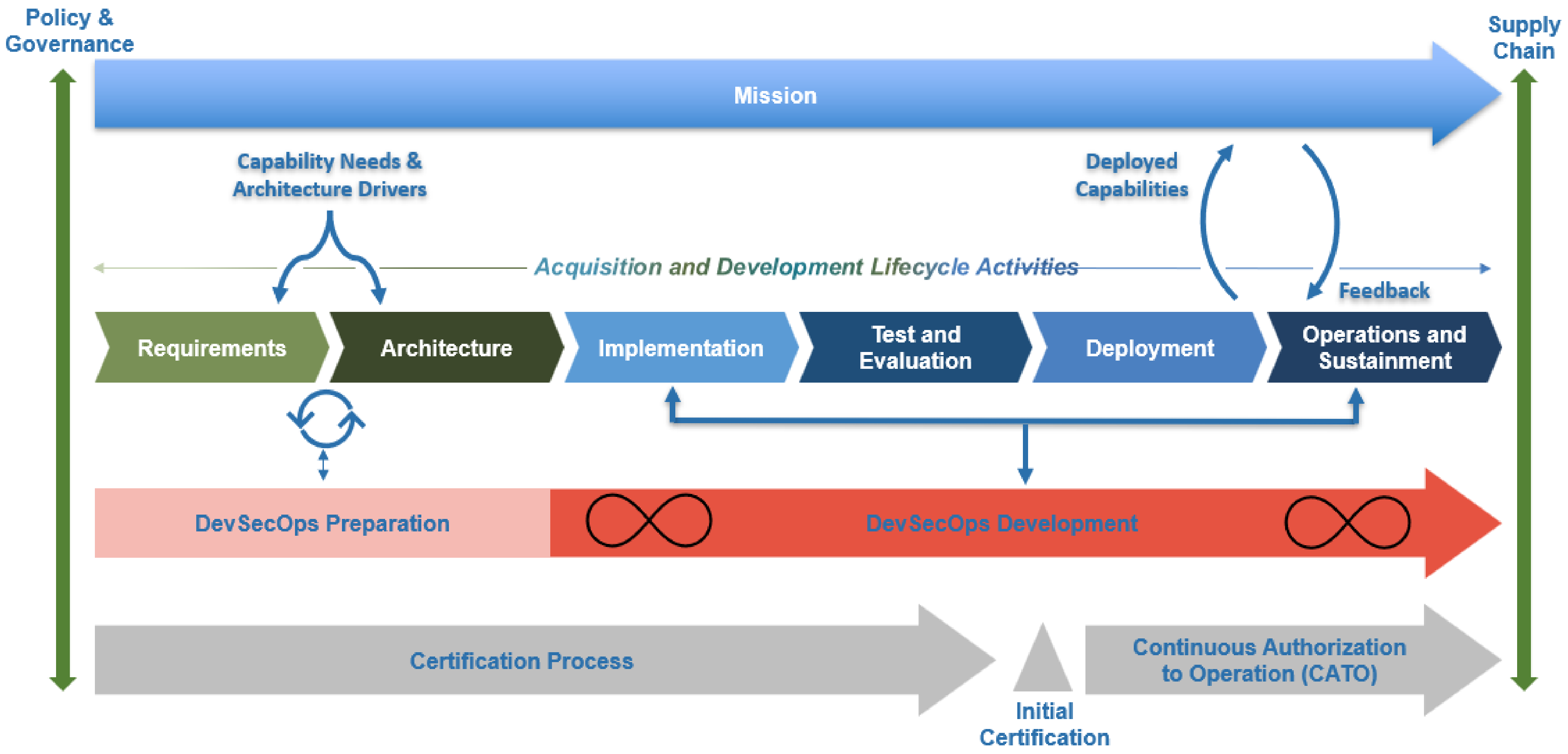
> ***“The B-52 lived and died on the quality of its sheet metal. Today our aircraft will live or die on the quality of our software.” —Air Force General***

Quote: “Delivering Military Software Affordably,” *Defense AT&L*, March-April 2013

There is lots of new guidance, but DoD programs are still functioning as they have for decades.

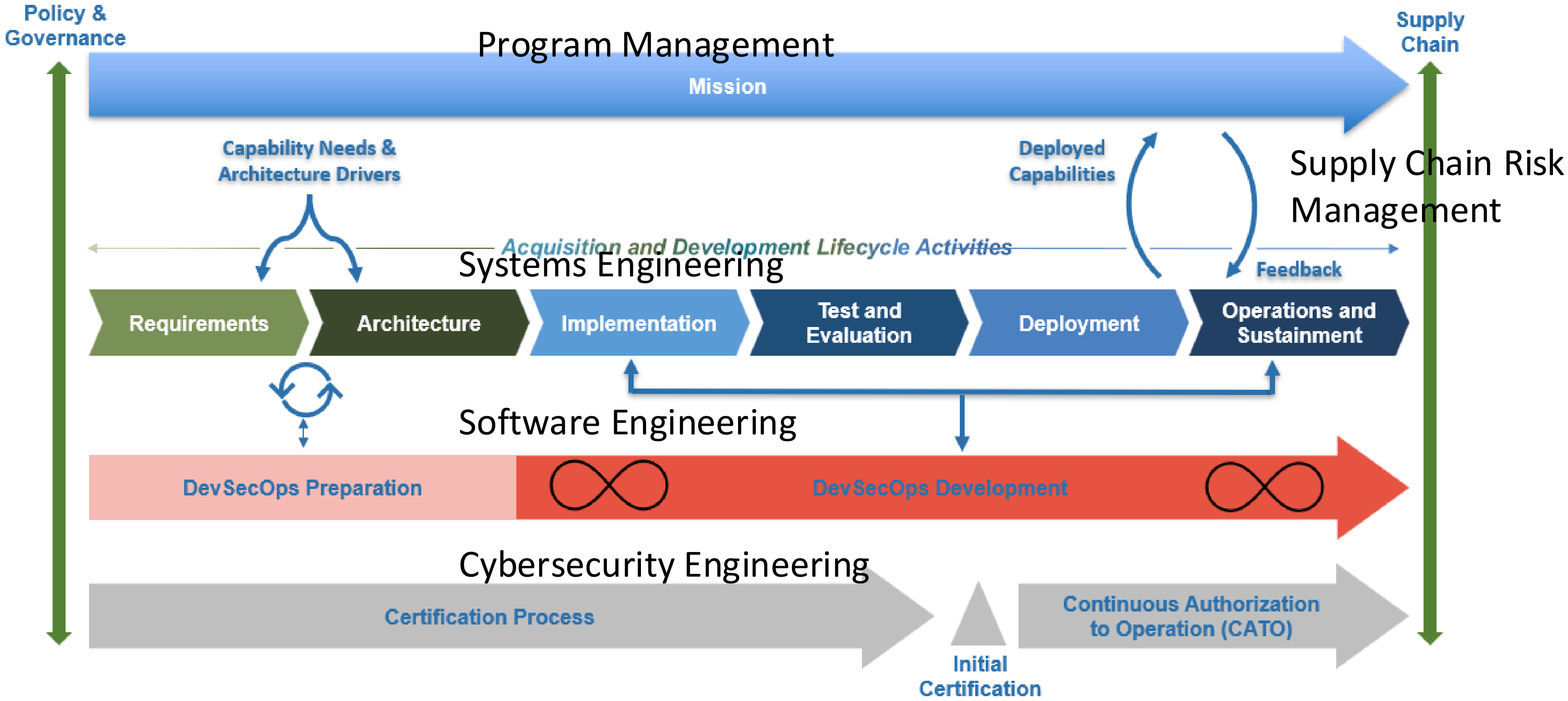
Current Acquisition Landscape in Disconnected

Carnegie Mellon University
Software Engineering Institute



DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution

Current Acquisition Landscape Divisions



Program Management

Systems Engineering

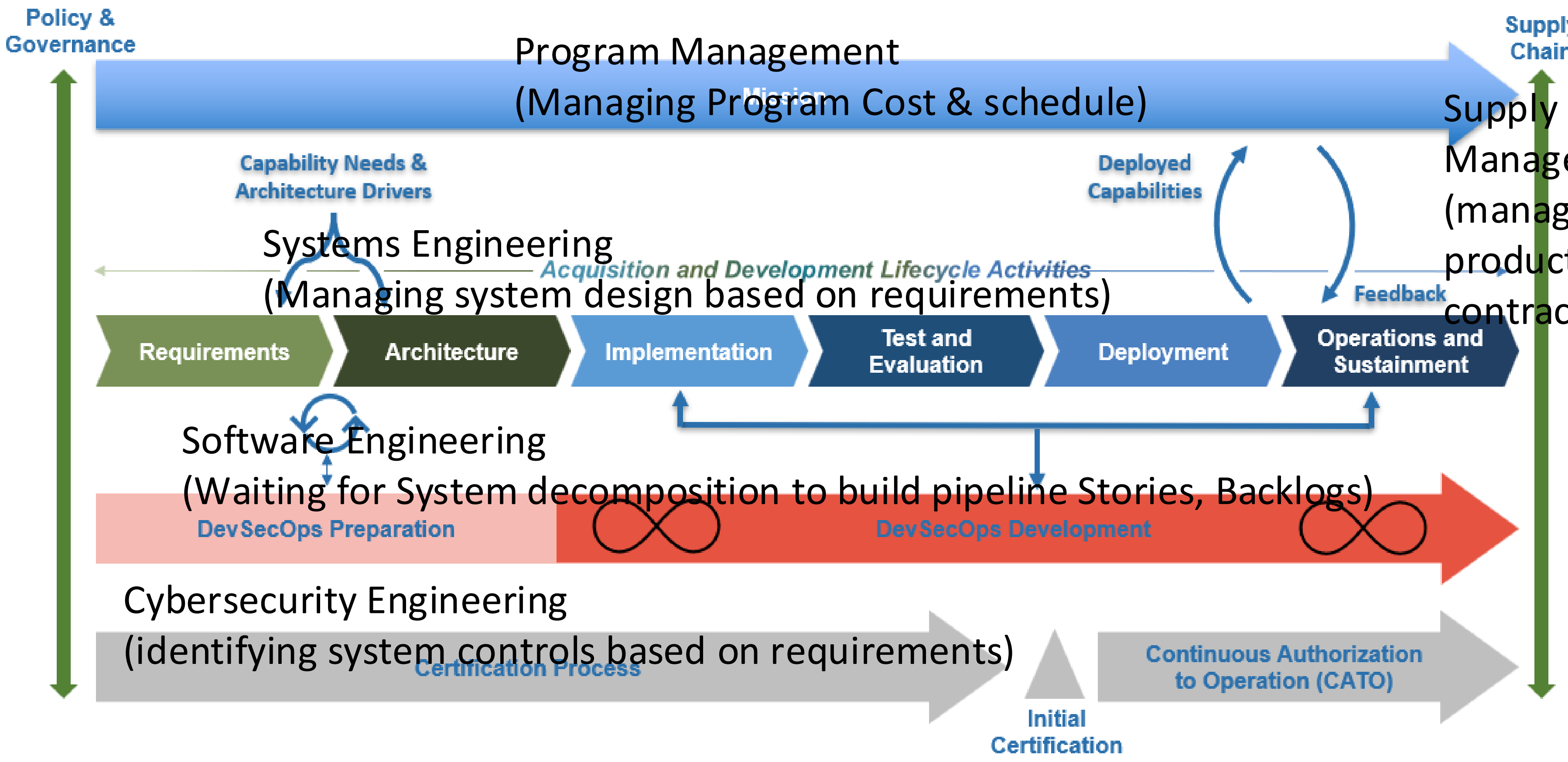
Software Engineering

Cybersecurity Engineering

Supply Chain Risk Management

DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution

Current Acquisition Landscape Subdivision Focuses



Program Management
(Managing Program Cost & schedule)

Supply Chain Risk Management (managing product contracts, cost)

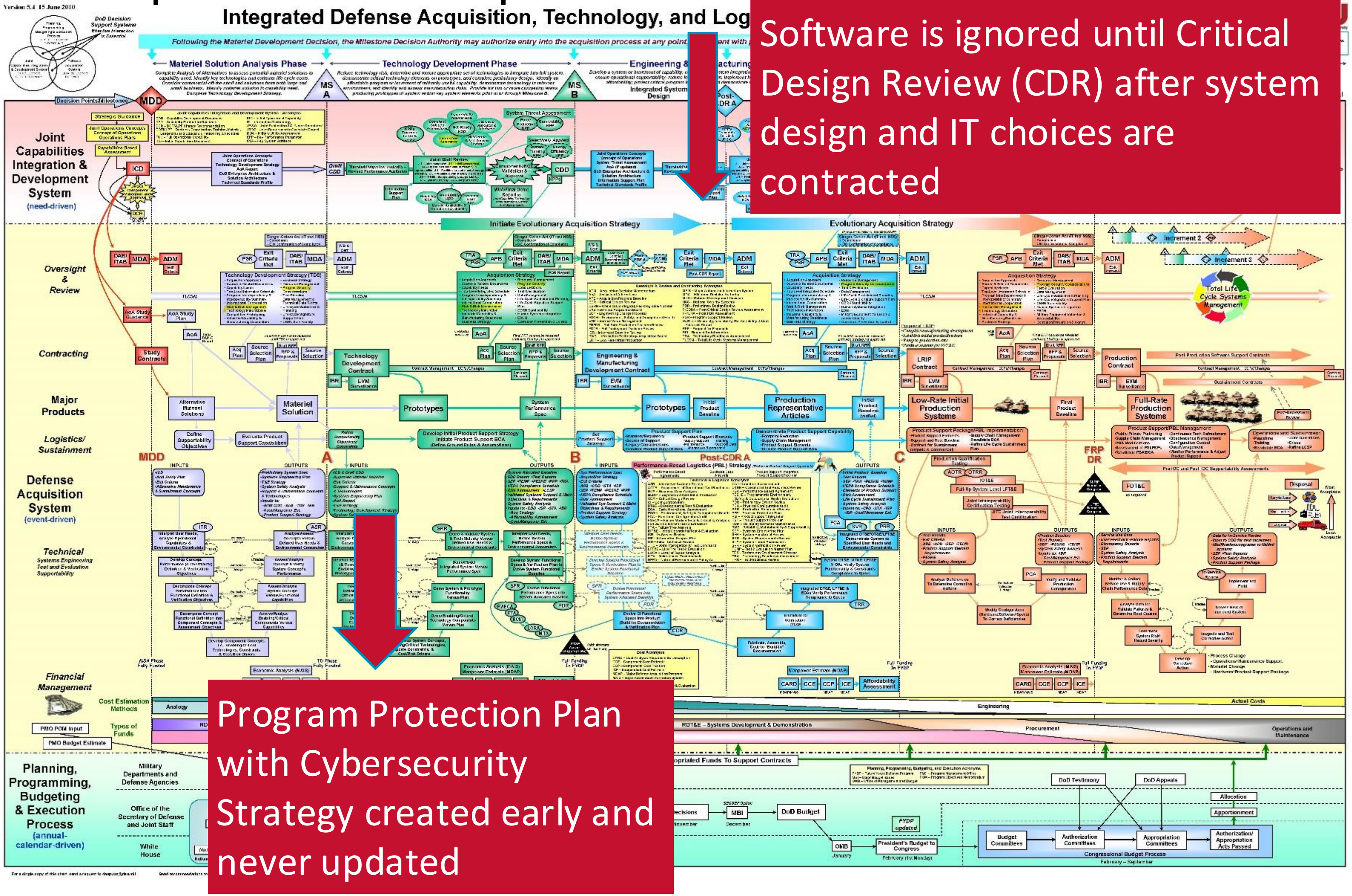
Systems Engineering
(Managing system design based on requirements)

Software Engineering
(Waiting for System decomposition to build pipeline Stories, Backlogs)

Cybersecurity Engineering
(identifying system controls based on requirements)

DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution

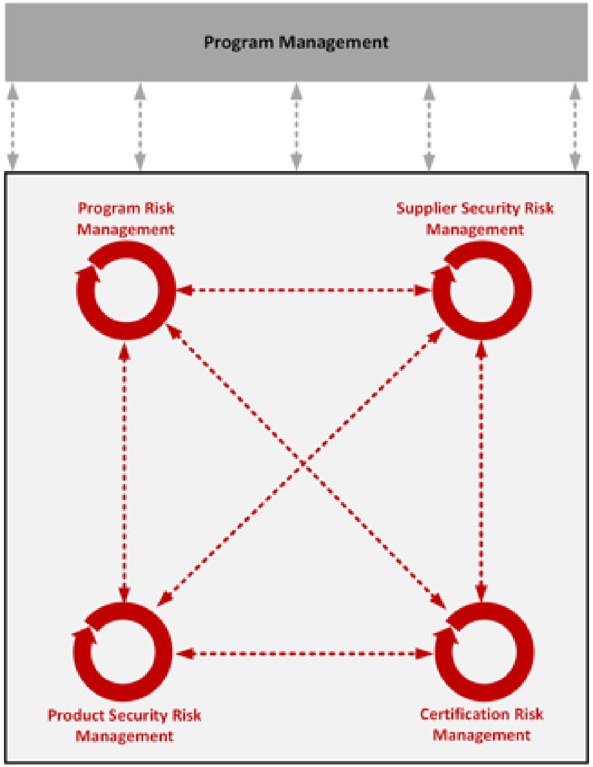
DoD Acquisition Process – Outputs and Verifications


Version 5.4 15 June 2010
Integrated Defense Acquisition, Technology, and Log
Following the Materiel Development Decision, the Milestone Decision Authority may authorize entry into the acquisition process at any point
Materiel Solution Analysis Phase
Technology Development Phase
Engineering &
MDD
MS A
MS B
Post-CDR A
Decision Points/Milestones
Joint Capabilities Integration & Development System
(need-driven)
Oversight & Review
Contracting
Major Products
Logistics/ Sustainment
Defense Acquisition System
(event-driven)
Technical
Systems Engineering
Test and Evaluation
Supportability
Financial Management
Planning, Programming, Budgeting & Execution Process
(annual-calendar-driven)
Initiate Evolutionary Acquisition Strategy
Evolutionary Acquisition Strategy
Increment 2
Increment 3
Total Life Cycle Systems Management
Technology Development Contract
Engineering & Manufacturing Development Contract
LRIP Contract
Production Contract
Materiel Solution
Prototypes
Production Representative Articles
Low-Rate Initial Production Systems
Full-Rate Production Systems
A
B
C
FRP DR
Disposal
Cost Estimation Methods
Types of Funds
PMO POM Input
PMO Budget Estimate
Engineering
Procurement
Operations and Maintenance
RDT&E – Systems Development & Demonstration
Actual Costs
Military Departments and Defense Agencies
Office of the Secretary of Defense and Joint Staff
White House
DoD Budget
MBI
OMB
President's Budget to Congress
DoD Testimony
DoD Appeals
Budget Committees
Authorization Committees
Appropriation Committees
Authorization/ Appropriation Acts Passed
Allocation
Apportionment
Congressional Budget Process

Software is ignored until Critical Design Review (CDR) after system design and IT choices are contracted

Program Protection Plan with Cybersecurity Strategy created early and never updated

Challenge: Integrating Security and Supply Chain Risk Management across the Organization


Program Management
Program Risk Management
Supplier Security Risk Management
Product Security Risk Management
Certification Risk Management

Security and supplier risk management are typically outside of the program risk management.

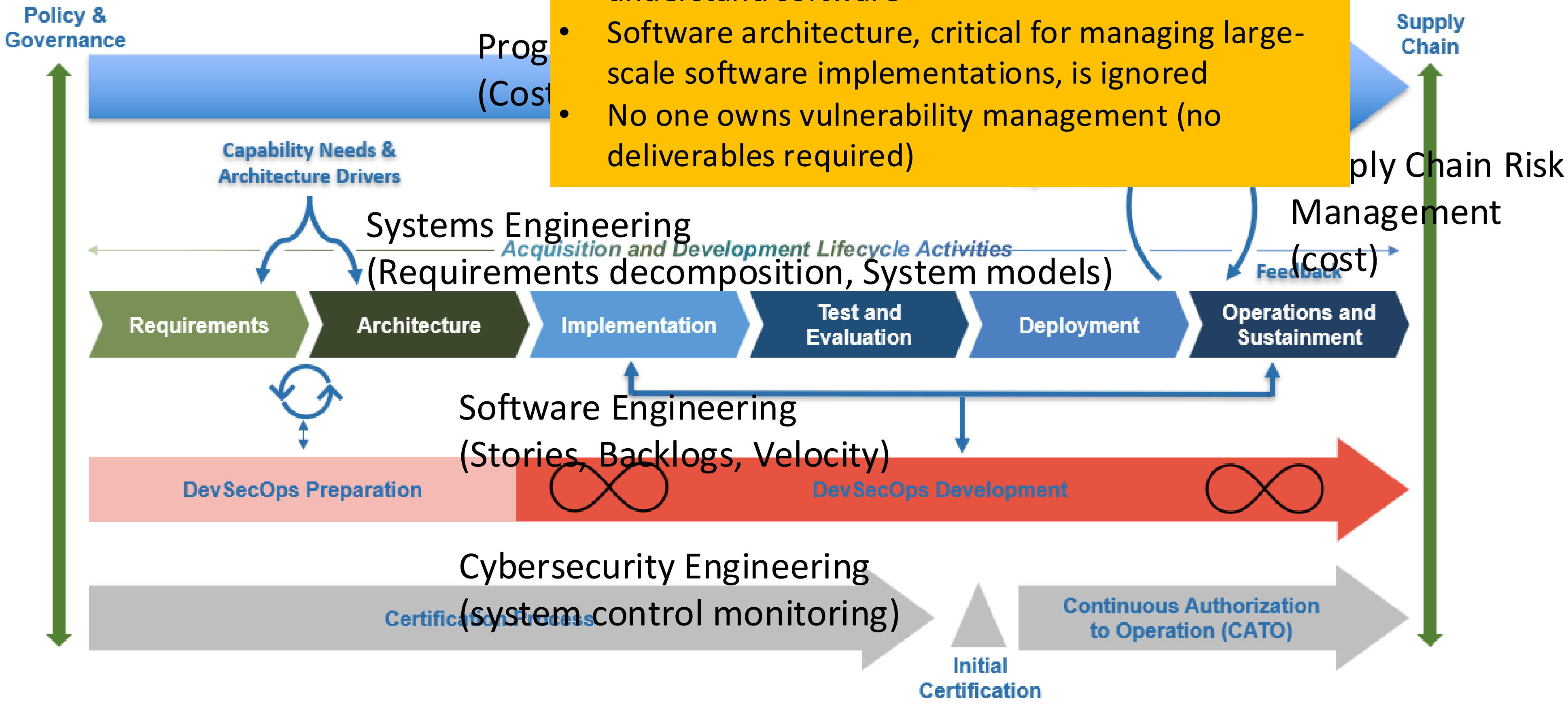
Information (such as it is) is scattered in many documents across the Acquisition such as Program Protection Plan (PPP), Cybersecurity Plan, System Development Plan, Supply Chain Risk Management Plan, etc.

Many activities across the organization are critical to managing cyber risks and must be addressed collaboratively across the lifecycle and supply chain and integrated with program risk management.

Current Acquisition Landscape Issues

Software assurance expertise is often missing:

- No one in the government owns code quality
- Supply chain management not staffed to understand software
- Software architecture, critical for managing large-scale software implementations, is ignored
- No one owns vulnerability management (no deliverables required)



Prog

(Cost

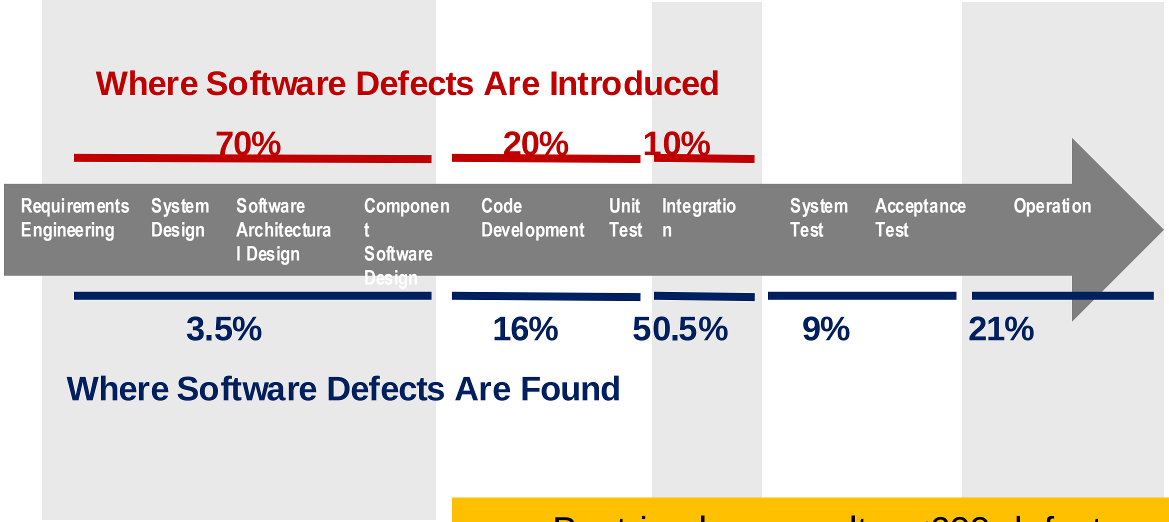
ply Chain Risk Management (cost)

Systems Engineering (Requirements decomposition, System models)

Software Engineering (Stories, Backlogs, Velocity)

Cybersecurity Engineering (system control monitoring)

All Software has Defects and Potential Vulnerabilities



Where Software Defects Are Introduced

70% 20% 10%

Requirements Engineering | System Design | Software Architectural Design | Component Software Design | Code Development | Unit Test | Integration | System Test | Acceptance Test | Operation

3.5% 16% 50.5% 9% 21%

Where Software Defects Are Found

Best-in-class results: <600 defects per million lines of code (MLOC)
Very good code: 600 to 1,000 defects per MLOC
Average quality code: 6,000 defects per MLOC

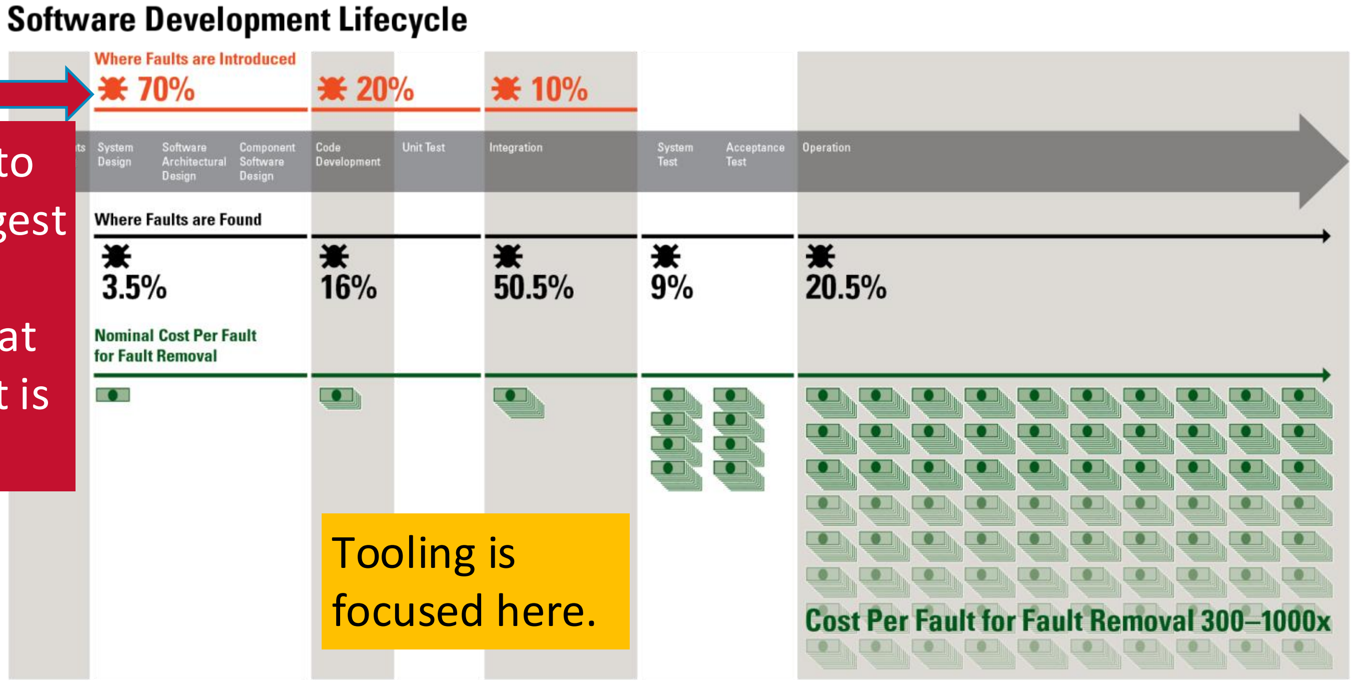
5% of these defects are potential vulnerabilities

Sources: *Critical Code*; NIST, NASA, INCOSE, and Aircraft Industry Studies;
Woody, C., Ellison, R., & Nichols, W. (2014). *Predicting Software Assurance Using Quality and Reliability Measures* (Report No. CMU/SEI-2014-TN-026). Software Engineering Institute, Carnegie Mellon University. https://insights.sei.cmu.edu/library/predicting-software-assurance-using-quality-and-reliability-measures-2/

Software Defects: *Introduction, Discovery, and Cost*

Defects account for 30–50% percent of total software project costs.

- Most are introduced before coding (~70%).
- Most are discovered at system integration or later (~80%).



Opportunities to reduce the largest volume of vulnerabilities at the lowest cost is lost

Tooling is focused here.

Software Assurance is an Unplanned Program Cost

New management and engineering approaches and skills are needed to produce assured software intensive products that

- Provide effective planning and oversite of software design, development, implementation & sustainment
- Identify and mitigate acquisition-related software security risks
- Plan for handling software risk management (resources, tools, risk identification)

Instead, programs continue to manage unchanged trying to fit the new elements into the existing processes and practices:

- Leadership is focusing only on system cost and schedule leaving software to later in the lifecycle
- Faulty assumptions that software never wears out so no funding for software reliability
- Missing skills and knowledge resources needed to identify and address software risks
- Lack of recognition that shifts to new technology require leadership education as well as technical experts

Summary

Carnegie Mellon University Software Engineering Institute

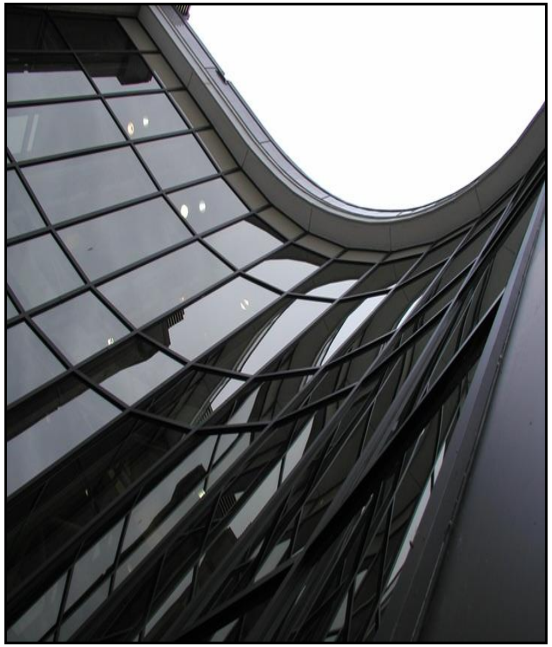
Change is Critical for Software Assurance

Expertise that understands software assurance, cybersecurity risk management, and software supply chain risk management must be highly integrated into decision making, design, development, and management of every lifecycle aspect.

- Current workforce will require major retraining to understand software and risk
- Incoming workforce is not learning this in school so the organization will have to train new hires
- Opportunities to improve software cost will require a focus on early lifecycle events

DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution

Contact Information



Carol Woody, Ph.D.

cwoody@cert.org

Web Resources

www.sei.cmu.edu/go/cybersecurity-engineering

http://www.sei.cmu.edu/

DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution