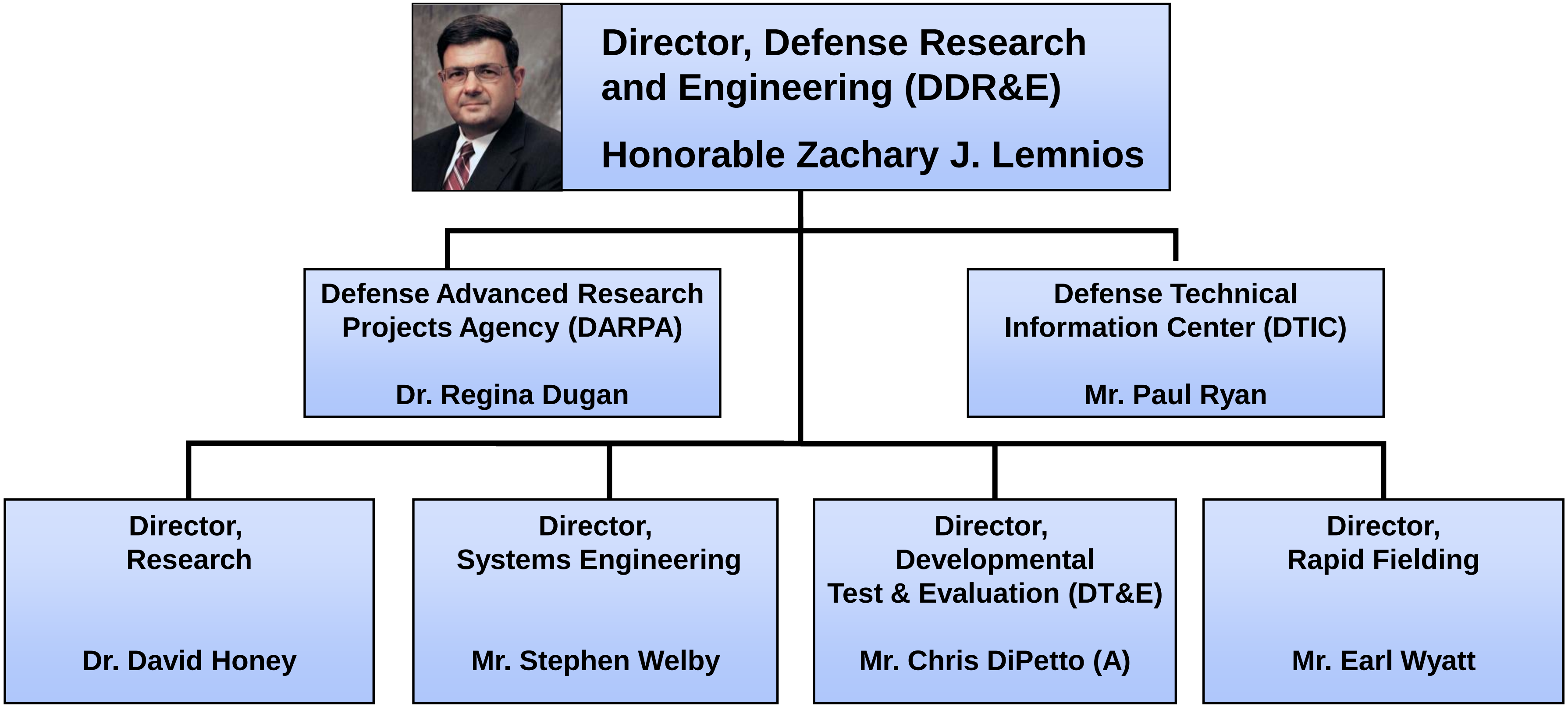
System Security Engineering

A Critical Discipline of SE

Ms. Kristen Baldwin
Director, Systems Analysis
DDR&E/Systems Engineering

12th Annual NDIA Systems Engineering Conference
28 October 2009

Defense Research & Engineering



Director, Defense Research and Engineering (DDR&E)

Honorable Zachary J. Lemnios

Defense Advanced Research Projects Agency (DARPA)

Dr. Regina Dugan

Defense Technical Information Center (DTIC)

Mr. Paul Ryan

Director, Research

Dr. David Honey

Director, Systems Engineering

Mr. Stephen Welby

Director, Developmental Test & Evaluation (DT&E)

Mr. Chris DiPetto (A)

Director, Rapid Fielding

Mr. Earl Wyatt

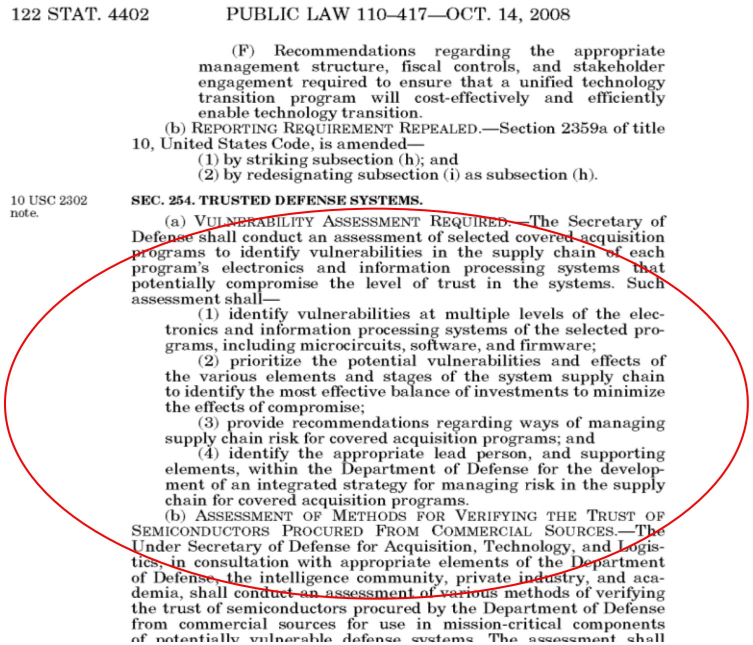
Increased Priority for Program Protection

- ***Threats*: Nation-state, terrorist, criminal, rogue developer who:**
  - Gain control of systems through supply chain opportunities
  - Exploit vulnerabilities remotely
- ***Vulnerabilities*: All systems, networks, applications**
  - Intentionally implanted logic (e.g., back doors, logic bombs, spyware)
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- ***Consequences*: Stolen critical data & technology; corruption, denial of critical warfighting functionality**

Today’s acquisition environment drives the increased emphasis:

Then		Now
Standalone systems	>>>	Networked systems
Some software functions	>>>	Software-intensive
Known supply base	>>>	Prime Integrator, hundreds of suppliers

Vulnerability Assessments



122 STAT. 4402 PUBLIC LAW 110–417—OCT. 14, 2008

(F) Recommendations regarding the appropriate management structure, fiscal controls, and stakeholder engagement required to ensure that a unified technology transition program will cost-effectively and efficiently enable technology transition.

(b) REPORTING REQUIREMENT REPEALED.—Section 2359a of title 10, United States Code, is amended—

(1) by striking subsection (h); and

(2) by redesignating subsection (i) as subsection (h).

10 USC 2302 note.

SEC. 254. TRUSTED DEFENSE SYSTEMS.

(a) VULNERABILITY ASSESSMENT REQUIRED.—The Secretary of Defense shall conduct an assessment of selected covered acquisition programs to identify vulnerabilities in the supply chain of each program's electronics and information processing systems that potentially compromise the level of trust in the systems. Such assessment shall—

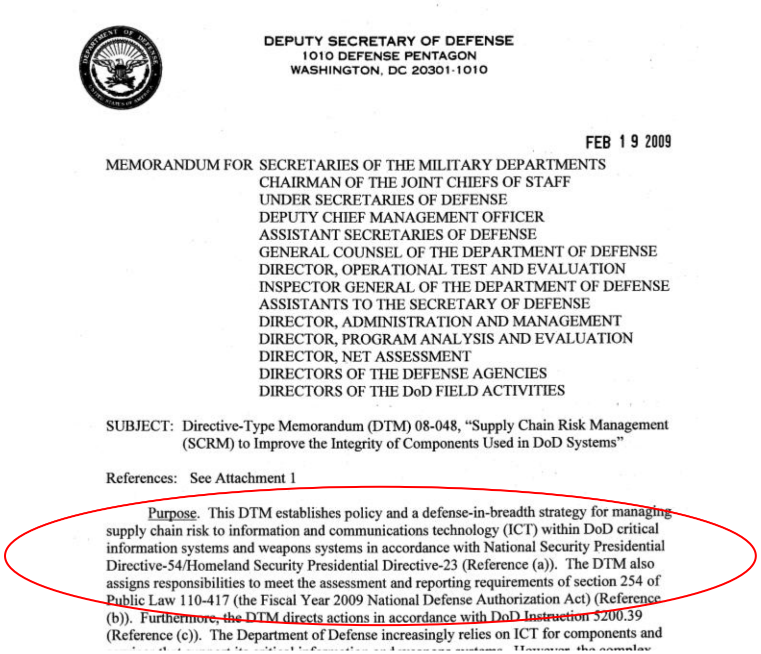
(1) identify vulnerabilities at multiple levels of the electronics and information processing systems of the selected programs, including microcircuits, software, and firmware;

(2) prioritize the potential vulnerabilities and effects of the various elements and stages of the system supply chain to identify the most effective balance of investments to minimize the effects of compromise;

(3) provide recommendations regarding ways of managing supply chain risk for covered acquisition programs; and

(4) identify the appropriate lead person, and supporting elements, within the Department of Defense for the development of an integrated strategy for managing risk in the supply chain for covered acquisition programs.

(b) ASSESSMENT OF METHODS FOR VERIFYING THE TRUST OF SEMICONDUCTORS PROCURED FROM COMMERCIAL SOURCES.—The Under Secretary of Defense for Acquisition, Technology, and Logistics, in consultation with appropriate elements of the Department of Defense, the intelligence community, private industry, and academia, shall conduct an assessment of various methods of verifying the trust of semiconductors procured by the Department of Defense from commercial sources for use in mission-critical components of potentially vulnerable defense systems. The assessment shall



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

FEB 19 2009

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

SUBJECT: Directive-Type Memorandum (DTM) 08-048, "Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems"

References: See Attachment 1

Purpose. This DTM establishes policy and a defense-in-breadth strategy for managing supply chain risk to information and communications technology (ICT) within DoD critical information systems and weapons systems in accordance with National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (Reference (a)). The DTM also assigns responsibilities to meet the assessment and reporting requirements of section 254 of Public Law 110-417 (the Fiscal Year 2009 National Defense Authorization Act) (Reference (b)). Furthermore, the DTM directs actions in accordance with DoD Instruction 5200.39 (Reference (c)). The Department of Defense increasingly relies on ICT for components and services that support its critical information and weapons systems. However, the complex

- **National Defense Authorization Act Section 254 – Directed DoD:**
  - **Perform vulnerability assessments of major systems**
- **Vulnerability Assessments**
  - **Supply chain review**
  - **Program protection planning review**
  - **System Engineering/In-depth design review**

- **Deputy Secretary of Defense Directive**
  - **Assigned "responsibilities to meet the assessment and reporting requirements of Section 254" of NDAA to ASD(NII)/DoD CIO and USD (AT&L)**

Vulnerability Assessment Highlights

- **Assessed 3 Major Defense Acquisition Programs**

- **Assessed 42 methods for verifying trust in commercial microelectronics**

- **Report to Congress in October 2009**
  - Summarizes assessment results, current DoD strategy, and way ahead
  - Demonstrates understanding of wider supply chain risk – not just microelectronics

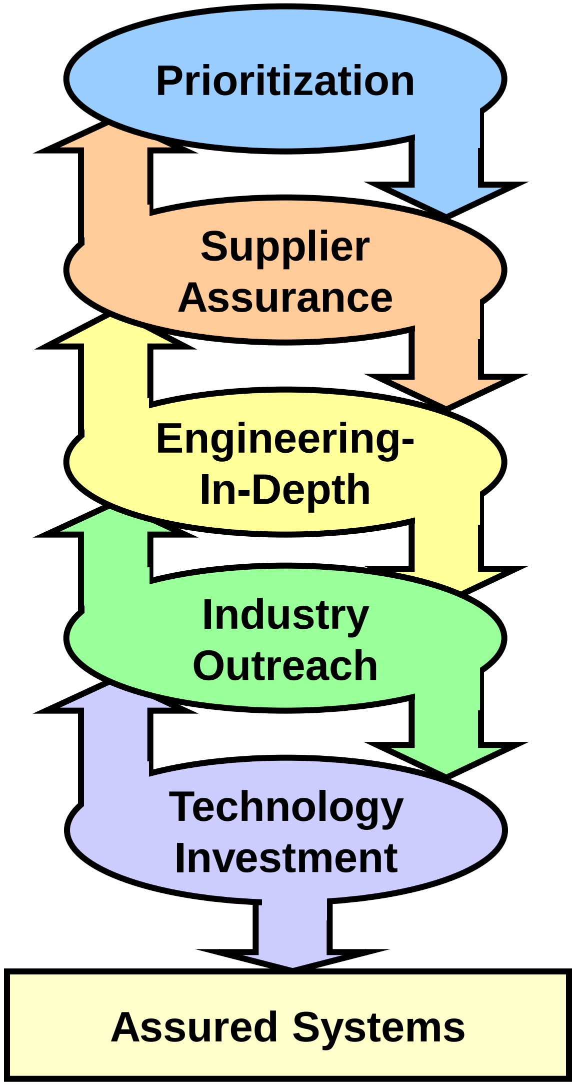
- **Recommended Actions**
  - Continue joint leadership by USD(AT&L) and ASD(NII)/DoD CIO
  - Address counterfeits during Logistics and Sustainment
  - Continue piloting mitigations with acquisition programs, implement findings in policy
  - Evaluate additional verification methods, including supplier management, inspections, and testing

Current Program Protection Challenges

- Policy and guidance for security is not streamlined
- There is a lack of useful methods, processes and tools for acquirers and developers
- Criticality is usually identified too late to budget and implement protection
- Horizontal protection process is insufficiently defined
- Lack of consistent method for measuring success of “protection”
- Security not typically identified as an operational requirement, and is therefore lower priority

Data Source: GAO report, white papers, military service feedback

Vision of Success



- The requirement for assurance is allocated among the right systems and their critical components
- Awareness of supply chain risks
- Systems are designed and sustained at a known level of assurance
- Commercial sector shares ownership and builds assured products
- Technology investment transforms the ability to detect and mitigate system vulnerabilities

DoDI 5200.39 Program Protection Policy

- **Perform comprehensive protection of Critical Program Information**
- **CPI includes elements or components of an RDA program that, if compromised, could:**
  - Cause significant degradation in mission effectiveness;
  - Shorten the expected combat-effective life of the system;
  - Reduce technological advantage;
  - Significantly alter program direction; or
  - Enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability
- **Includes information about applications, capabilities, processes, and end-items**
- **Includes technology that would reduce the US technological advantage if it came under foreign control**
- **Includes elements or components critical to a military system or network mission effectiveness**

-DoDI 5200.39

Protection Disciplines: Some Definitions

- **Information Assurance: Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation** *(DoD 8500.01E: Information Assurance)*
- **Cyber Security: Measures taken to protect a computer, networks, or information or computer system (as on the internet) and electronic information storage facilities belonging to, or operated by or for, the DoD or US Government, against unauthorized access, or attack, or attempts to access** *(DoDI 5205.ff: Defense Industrial Base Cyber Security/Information Assurance Activities)*
- **System Assurance: 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** *(NDIA Engineering for System Assurance Guidebook)*
- **System Security Engineering: An element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities** *(MIL-HDBK-1785: System Security Engineering Program Management Requirements)*

A Comparison

System Assurance

- **Protects: Critical Program Information**
- **Format: End-items, critical components, integrated circuits, field programmable gate arrays, embedded software, etc.**
- **Purpose: Through design, builds in safeguards, resistance, redundancy, and intrinsic strength**
- **Verification: Systems engineering and test procedures; system security engineering**

Information Assurance/Cyber Security

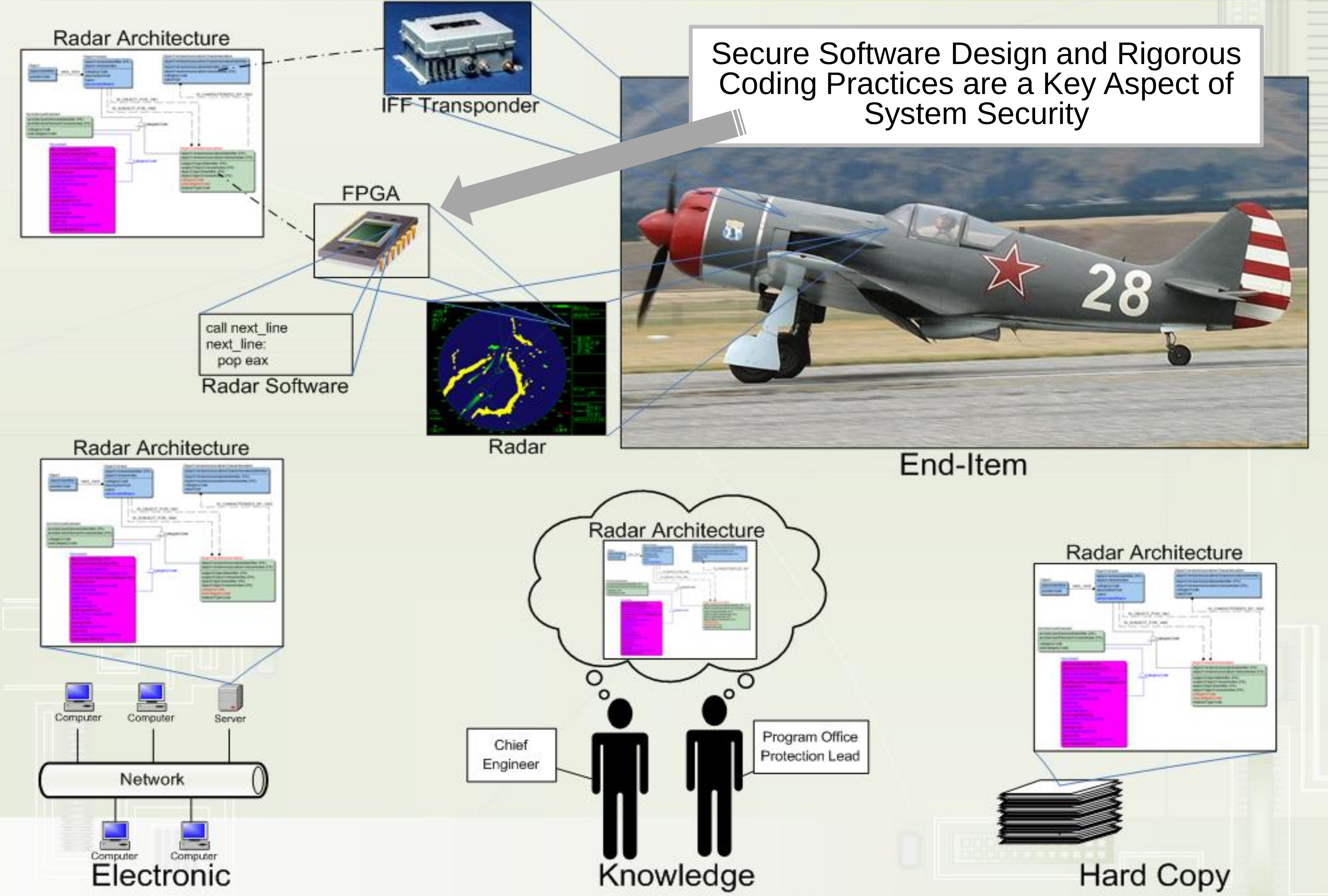
- **Protects: Protects any information/ functionality, *not specific to CPI***
- **Format: Applications, networks, IT processes, platform IT interconnections (includes weapon systems)**
- **Purpose: Standardizing strong network security and system administration practices**
- **Verification: DIACAP**

CPI Protection Example: Aircraft Radar Architecture and Waveform

- **What are the formats/locations of the information?**
  - **End-items (hardware and software), Information Systems (networks, applications), Human Knowledge, Hard Copy Documents**
- **How is the information protected in those formats?**
  - **Countermeasures and verifications vary by format**

System Security Engineering is Required to Cost Effectively Design-In CPI Protection

Secure Software Design and Rigorous Coding Practices are a Key Aspect of System Security



```
call next_line
next_line:
  pop eax
```

Notional Diagram – Does not illustrate actual locations of CPI or components of any aircraft

CPI Formats and Example Protections

- **Information Systems**
  - Information Assurance (controls for applications, networks, IT processes and platform IT interconnections)
  - Communications Security (Encryption, decryption)

- **Hard Copy Documents**
  - Information Security (Document markings, handling instructions)
  - Foreign Disclosure (restrict/regulate foreign access)
  - Physical Security (gates, guards, guns)

- **End Items**
  - Anti-Tamper (deter, prevent, detect, respond)
  - Information Assurance
  - Supply Chain Risk Management (assessing supplier risk)
  - Software Assurance (tools, processes to ensure SW function)
  - System Security Engineering
  - Trusted Foundry (integrated circuit providers)

- **Ideas/Knowledge**
  - Personnel Security (trustworthy, reliable people)
  - Access Controls

UNCLASSIFIED

System Security Engineering

- **Security Specialties have evolved overtime in response to threats:**
  - Information Security
  - Computer/Network Security
  - Physical Security
  - Information Systems Security
- **The above specialties do not adequately address end-item threats**
- **Much work is needed to fully expand this discipline**
  - Foundational science and engineering, competencies (as compared to other SE Specialties: reliability, safety, etc)
  - Methods and tools: V&V, architecting for security
  - Community and design team recognition of SSE as a key design consideration
- **INCOSE has chartered a System Security Engineering Working Group that can take on many of these challenges**
- **The SE Research Center (SERC) is defining a SSE Research Initiative**

Our Challenge: Protection Hard Problem List

- **CPI identification, and duration (years) of protection required**
- **Identification of attack vectors (vulnerabilities)**
- **Quantifying the amount of Protection needed to reduce program risk**
  - Cost of protection countermeasures vs security risk to CPI
  - Effectiveness of protection throughout life cycle
- **Measuring effects/false alarm rates as part of system design**
- **New Protection Mechanisms, Tools**
  - Technologies to improve protection available to programs (Anti-Tamper, Software Assurance, Integrated Circuit pedigree, etc.)
  - Tools to test and assess system assurance
  - Methodologies for assessing assurance level

Questions?

DODD 8500.01E: Information Assurance

- **Information assurance requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DoD information systems**
- **For IA purposes all DoD information systems shall be organized and managed in four categories:**
  - Automated information system (AIS) applications,
  - Enclaves (includes networks),
  - Outsourced IT-based processes, and
  - Platform IT interconnections (includes weapon systems)

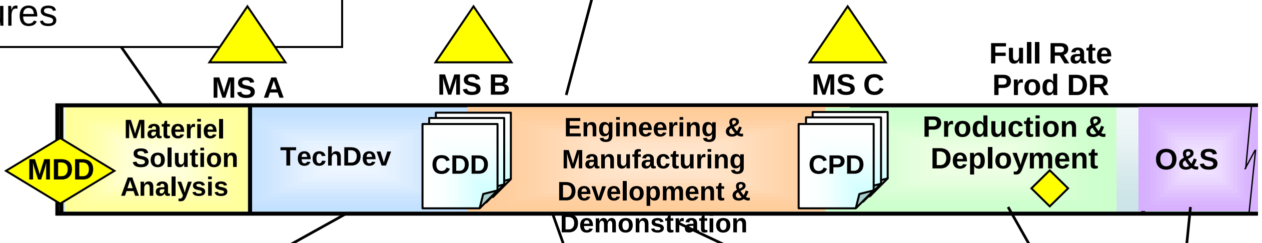
Early, Designed-In Program Protection

- Acquisition Strategy, **TDS**, RFP, SEP, and TEMP must be revised to include PPP relevant information
- **Milestone Decision Authority approves PPP in addition to PM**

Streamlined Program Protection Plan

- **One-stop shopping for documentation of acquisition program security (ISP, IAS, AT appendices)**
- **Living document, easy to update, maintain**
- **Improve over time based on feedback**

- Identify draft CPI, estimated protection duration and S&T Lab countermeasures

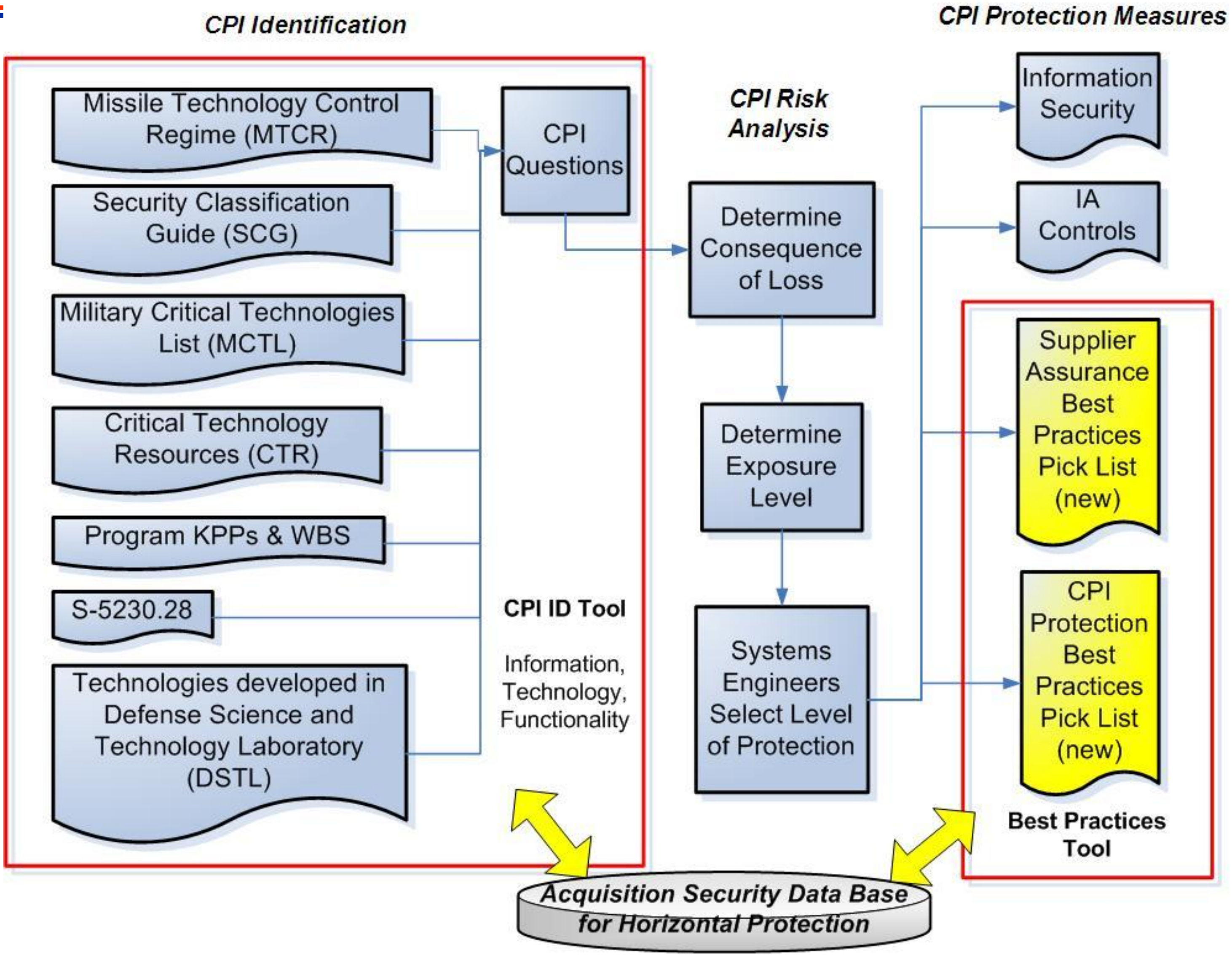

MS A
MS B
MS C
Full Rate Prod DR
MDD
Materiel Solution Analysis
TechDev
CDD
Engineering & Manufacturing Development & Demonstration
CPD
Production & Deployment
O&S

- Obtain threat assessments from Intel/CI, assess supplier risks
- Develop design strategy for CPI protection
- **Submit PPP to Acquisition Security Database (ASDB)**

- Contractor adds detail to Program Protection Plan
- Preliminary **verification and validation** that design meets assurance plans

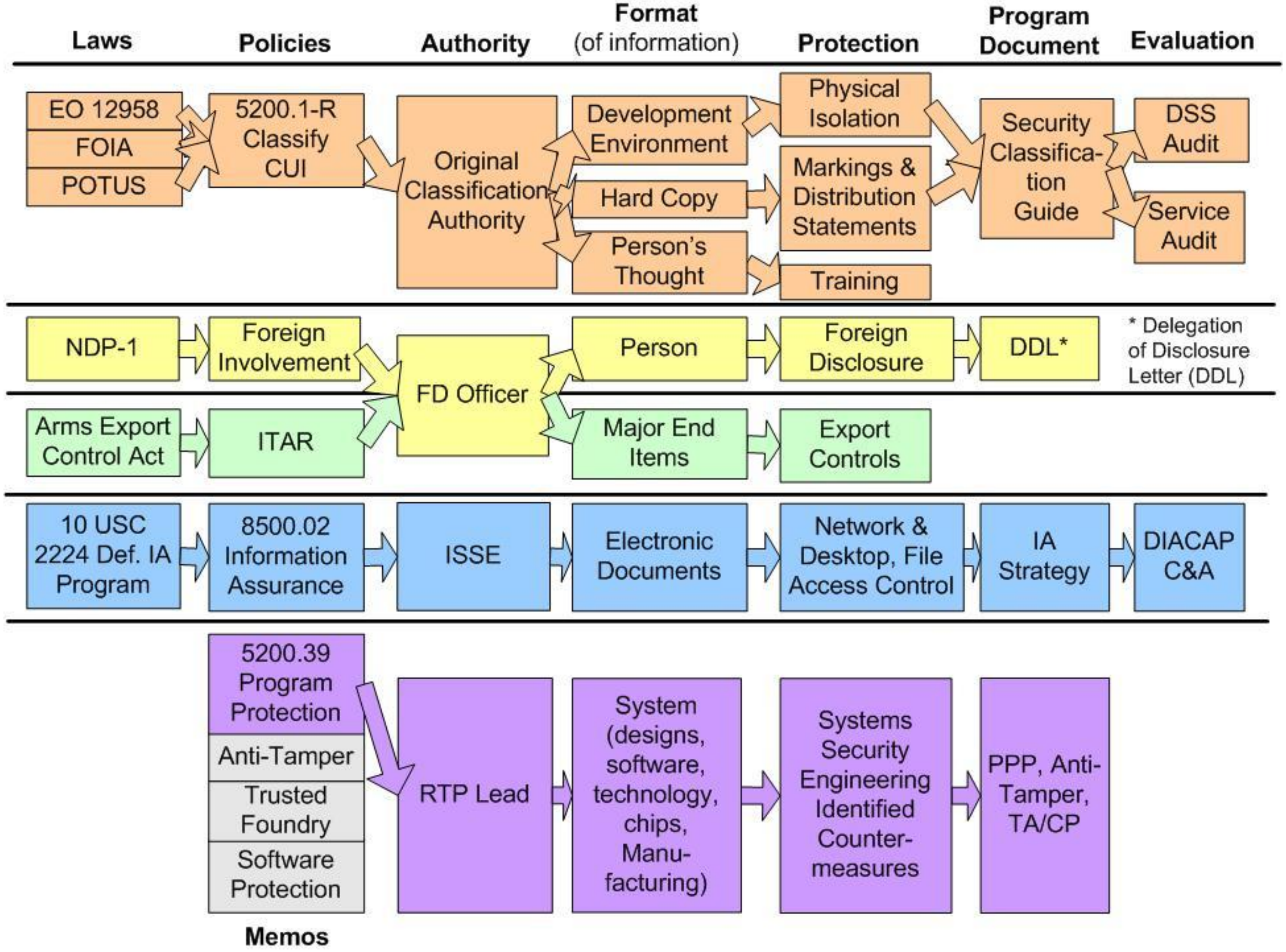
- Enhance countermeasure information in Program Protection Plan (PPP)
- **Evaluate** that CPI Protection RFP requirements have been met

Program Protection Tools


CPI Identification
CPI Protection Measures
Missile Technology Control Regime (MTCR)
Security Classification Guide (SCG)
Military Critical Technologies List (MCTL)
Critical Technology Resources (CTR)
Program KPPs & WBS
S-5230.28
Technologies developed in Defense Science and Technology Laboratory (DSTL)
CPI Questions
CPI ID Tool
Information, Technology, Functionality
CPI Risk Analysis
Determine Consequence of Loss
Determine Exposure Level
Systems Engineers Select Level of Protection
Information Security
IA Controls
Supplier Assurance Best Practices Pick List (new)
CPI Protection Best Practices Pick List (new)
Best Practices Tool
Acquisition Security Data Base for Horizontal Protection

18

OLD: Stovepipe Security (5 of 120 policies shown)



Laws | Policies | Authority | Format (of information) | Protection | Program Document | Evaluation

EO 12958
FOIA
POTUS
5200.1-R Classify CUI
Original Classification Authority
Development Environment
Hard Copy
Person's Thought
Physical Isolation
Markings & Distribution Statements
Training
Security Classification Guide
DSS Audit
Service Audit

NDP-1
Foreign Involvement
FD Officer
Person
Foreign Disclosure
DDL*

* Delegation of Disclosure Letter (DDL)

Arms Export Control Act
ITAR
Major End Items
Export Controls

10 USC 2224 Def. IA Program
8500.02 Information Assurance
ISSE
Electronic Documents
Network & Desktop, File Access Control
IA Strategy
DIACAP C&A

5200.39 Program Protection
Anti-Tamper
Trusted Foundry
Software Protection
Memos
RTP Lead
System (designs, software, technology, chips, Manufacturing)
Systems Security Engineering Identified Countermeasures
PPP, Anti-Tamper, TA/CP

Path Forward

- **Create a policy ‘framework’ to link multiple security disciplines**
- **Leverage and implement Program Protection Planning policy**
  - Link with acquisition oversight and program management processes
  - Provide training and support
  - Establish horizontal protection procedures
- **Augment system engineering guidance and practice to implement protection throughout lifecycle**
  - “Engineering for System Assurance” v1.0 Guidebook http://www.acq.osd.mil/sse/ssa/guidance.html

Raise the bar:	
Awareness	- Knowledge of the supply chain - Who has access to our critical assets
Protection	- Protect critical assets through security - Engineer our systems for assurance