The Globalization Challenge for Trusted Systems, and DoD Response

Mr. Mitchell Komaroff
Director, Globalization Task Force
OASD(NII)/DoD CIO

Agenda

- Globalization Challenge
- DoD Response
  - DoD Software and Systems Assurance CONOPS
  - DODI 5200.39, “Critical Program Information Protection Within the DoD”
  - Key DoD IA Programs to meet the Challenge
- Supply Chain Risk Management
  - Strategy
  - Technical Toolkit
- DoD Way ahead

Globalization Challenge

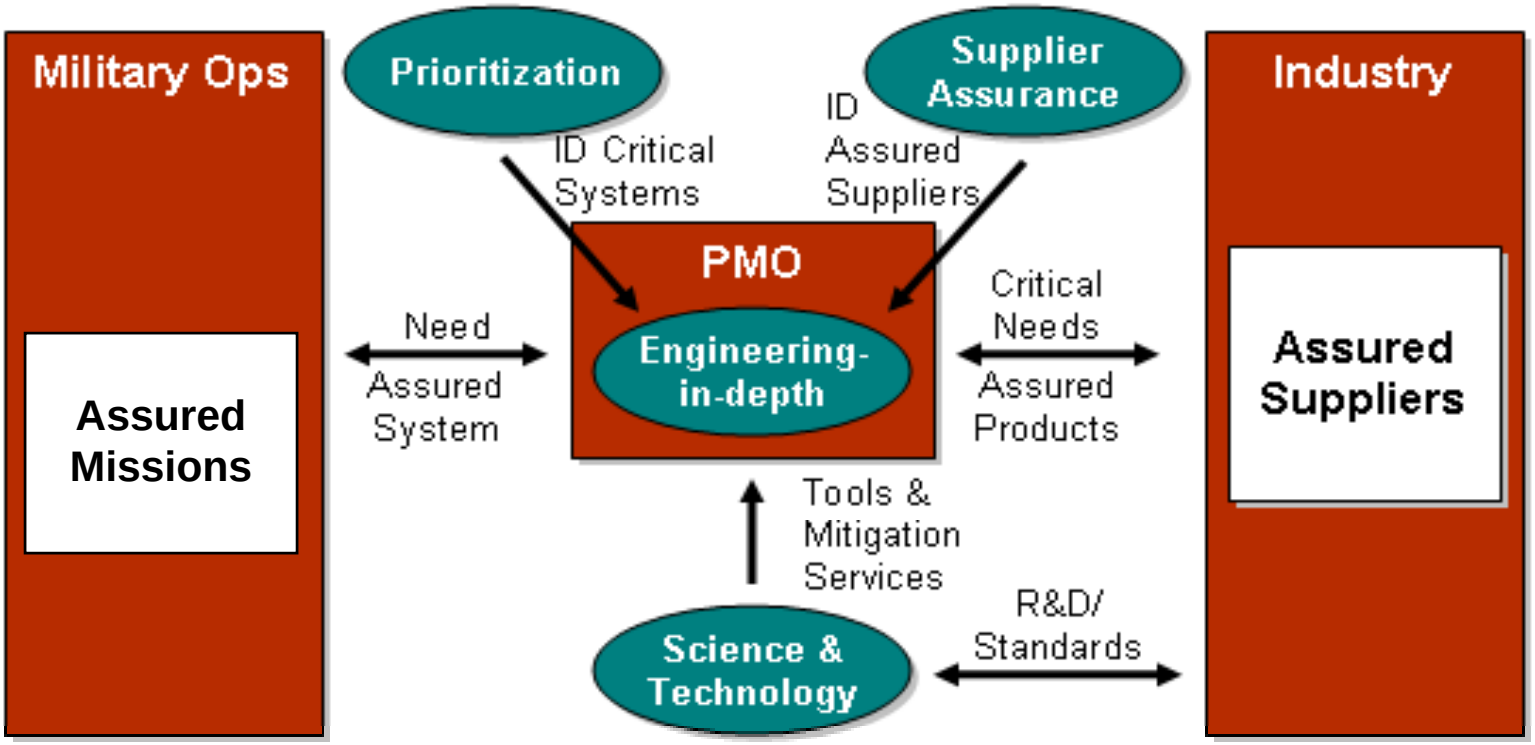
- Commercial IT functionality has penetrated nearly every aspect of DoD Mission Critical Functionality
  - Dramatically varying quality, reliability and trustworthiness
- IT communications connects nearly all DoD IT functionality together and with the functionality of the rest of the world *including our adversaries*
- IT Supply Chain is global, no longer under US control and is increasingly not trusted
  - Competitors and adversaries actively participating in the supplier chain

DoD weapons and command and control systems must be robust against full spectrum of attacks to achieve mission assurance

Sophisticated Nation-state Adversary

- Employ a full spectrum of offensive capabilities
  - Deep knowledge of latent vulnerabilities
  - Supply chain attacks to create vulnerabilities
- Don't "play fair"
  - Use systems approach to identify target of attack
  - Wait for time and place convenient to themselves
  - Insiders, surreptitious entry, etc.
- Individual target difficult to defend against determined Nation-state Adversary case-by-case

DoD Systems/Software Assurance CONOPS



The strategy components interact with operations, acquisition, and industry to produce assured systems

DODI 5200.39 "Critical Program Information Protection Within the DoD"

- It is DoD Policy:
  - To provide uncompromised and secure military systems to the warfighter by
    - performing comprehensive protection of CPI
    - through the integrated and synchronized application of CI, Intelligence, Security, systems engineering, and other defensive countermeasures to mitigate risk…
  - To minimize the chance that the Department's warfighting capability will be impaired due to the compromise of elements or components being integrated into DoD systems by foreign intelligence, foreign terrorist, or other hostile elements *through the supply chain or system design*.

DODI 5200.39: Critical Program Information

- **"CPI. Elements or components of an RDA program that, if compromised, could cause significant degradation in mission effectiveness;**

…

  - **Includes information about applications, capabilities, processes, and end-items.**
  - ***Includes elements or components critical to a military system or network mission effectiveness.***
  - **Includes technology that would reduce the US technological advantage if it came under foreign control…"**

DoD IA Strategic Plan
Operationalizing the IA Baseline

Vision: **TRUSTED INFORMATION—ANYTIME, ANYWHERE**

Operations

Goal: Achieve Mission Assurance

- Secure the Core Networks
- Trusted Information Sharing
- Assured Weapons Platforms

Technology

Goal: Protect Information

- Cross Domain Solutions
- Data at Rest—Data in Motion
- Key & Identity Management
- Trusted Computing/High Assurance Platform
- Deploy Protection Capabilities

Goal: Defend Systems & Networks

- Federal Desktop Core Configuration
- Insider Threat Mitigation
- Enterprise CND Tools & Capabilities
- CND Enterprise Sensor Grid

Processes

Goal: Transform & Enable IA Capabilities

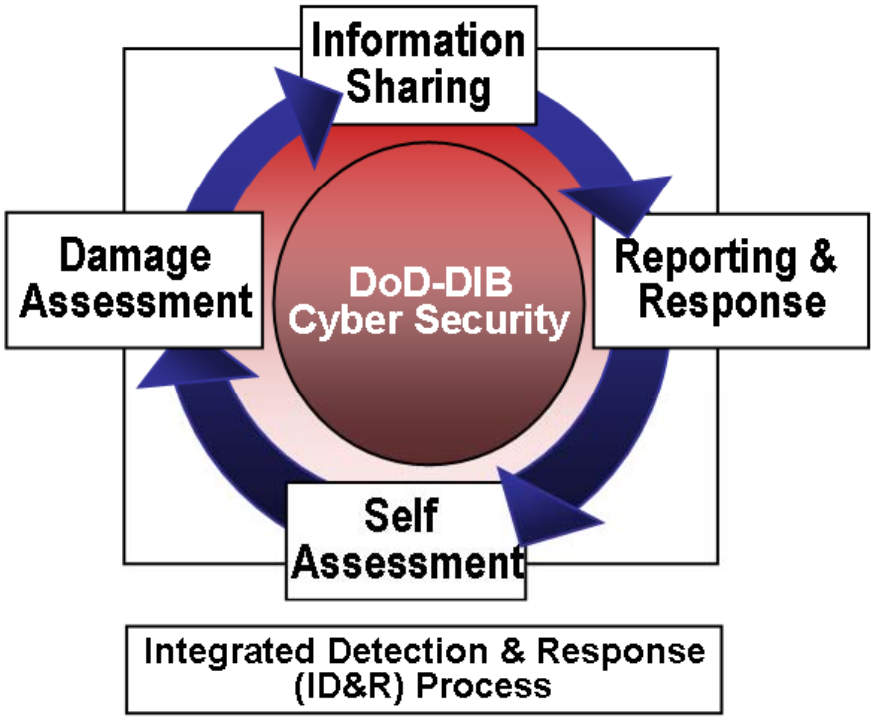
- IA/Cyber Architecture
- Defense Industrial Base IA
- International & Research Programs
- GIG Mission Assurance
- Globalization Task Force

People

Goal: Create an IA Empowered Workforce

- Certification
- Workforce Management
- Training Enhancement
- IA Outreach
- Benefits Realization

Defense Industrial Base Integrated Detection & Response Process



- Collaborative effort by DoD and DIB Partners involves:
  - Office of DOD-DIB Collaborative Information Sharing Environment (DCISE) at DoD's Cyber Crime Center is focal point for DIB
  - Multiple Government Agencies integrated into DCISE, providing best practices, expertise and information
- Construct contained in the Framework Agreement and implementing CONOPS

DIB IA Update

- Phase I
  - Critical Infrastructure Partnership Advisory Council IAWG
  - "Volunteer Phase" to assess DIB situation and DoD/DIB collaboration mechanisms
  - Evaluating DIB IA Capability Benchmark (set of IA Best Practices)
- Phase II: Acquisition and Contracting
  - Part 1- Immediate steps to begin protecting Controlled Unclassified Information
    - Interim Policy Memo to Component Acquisition Executives (CAEs)
  - Part 2 - Provides DOD empirical basis for evaluating best approach for permanent solution (DFARS or FAR)
    - OSD and CAEs to select several FY08 programs to pilot
    - Willing Industry partners also solicited

DoD Globalization Task Force

- **GTF Mission:** To develop and oversee implementation of a strategy for mitigating national security risks to DoD systems and networks arising from the globalization challenge

- **GTF Programs**:
  - Transactional Risk Management (CFIUS, FCC, etc)
  - Strategic Supply Chain Risk Management
  - Systems Assurance
    - Software Assurance
    - Trusted Foundry/Trusted Access Program Office

- **GTF Strategic Linkages:**
  - Defense Industrial Base Cyber Security Task Force
  - Global Information Grid Mission Assurance

Supply Chain Risk Management (SCRM)

Gaps in the CFIUS approach

- CFIUS is limited to direct investment
  - Does not address full lifecycle; Ownership is not the key to the introduction of vulnerabilities and risk
  - Does not include strategic partnerships, outsourcing/offshoring agreements or service level agreements
- Products and Services provided by U.S. companies often developed and managed overseas

About SCRM

- Provide the USG with a robust toolset to better manage and mitigate global ICT supply chain risk to their systems and networks
  - Considers criticality and risk of the technology and acquisition environment
  - Provides toolset of acquisition, technical and intelligence resources to be used across the entire lifecycle
- Complements and enriches current CFIUS process

SCRM Guiding Principles

- Defense-in-breadth: Mitigate risk across the entire lifecycle
- Understand risk management problem from a systems perspective
  - Response should be commensurate with risk and system/network criticality
  - Need to understand levels of vulnerability and threat relative to each system
- Drive higher assurance characteristics into commercial products where we have leverage
- Continued access to global ICT is critical to DoD mission

Sample Lifecycle Management Strategy

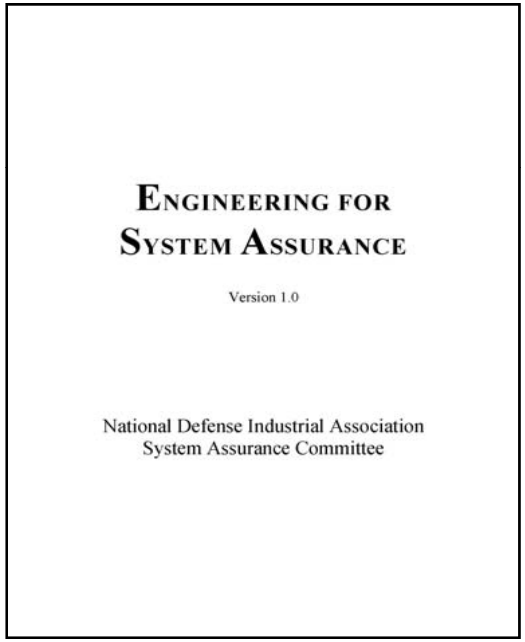
Life Cycle Phases	Design	Manufacturing	Integration	Distribution	Operations	Services/ Maintenance	Retirement
Sample Protective Measures	• Identify critical components early •Use isolation and separation	• Employ service level agreements related to quality and security •Trusted suppliers	• Limit online SW installations •Thoroughly vet updates	• Use secure distribution channels	• Implement and enforce traditional information assurance policies	• Confirm the integrity of network mapping	•Secure destruction of media and computers
	← To meet tomorrow's threat we must develop protection measures across product lifecycle *and* reinforce these measures through USG acquisition processes and effective implementation of agency security practices →						

DoD Defense-in-Breadth Technical Toolbox: Systems Assurance

- Systems Engineering Guidance for Systems Assurance
  - Identifies critical components for enhanced protection
  - Maps ISSE, Anti-tamper/software protection, program protection planning to DoD acquisition/systems engineering lifecycle
- Trusted Access Program Office/Trusted Foundry
  - Provides leading-edge DoD application specific integrated circuits (ASIC) from cleared foundries
- Software Assurance and Enhanced Test and Evaluation
  - NSA Center for Assured Software
  - CWE Formalization Demonstration

Engineering for Systems Assurance

- Developed by AT&L and NII through NDIA Systems Assurance Committee
- Scope
  - All within the context of system and software lifecycles
  - Assurance of security
  - Management of risk
- Intent of the Guidebook: Provide practical guidance augmenting systems engineering with systems assurance practices
  - Provide knowledge for applying technical assurance measures within ISO 15288 systems engineering technical process
- Guidance developed using DoD Lifecycle Framework
  - Guidance for each technical review within the lifecycle
  - "Proto-checklist" level of detail
  - Built IA, program protection, Anti-tamper into lifecycle, as they pertain to and enforce system assurance
- Accomplishments:
  - First order: Delivered reasonable security and assurance engineering practices to achieve robustness
  - Second order: started addressing element criticality, building an assurance case and measurement


ENGINEERING FOR
SYSTEM ASSURANCE

Version 1.0

National Defense Industrial Association
System Assurance Committee

Challenges in Developing SA Guidance

- Defining System Assurance
- Addressing Criticality
  - System and component
  - Minimizing the need for critical components
- Defining a notional concept of an Assurance Case
  - What makes up an assurance case?
  - Drawing out indicators/measures to build a system assurance case in the system lifecycle
- Bringing a balanced focus on both software and hardware
- Balancing out guidance for system integrators vs. COTS vendors

Definition of System Assurance

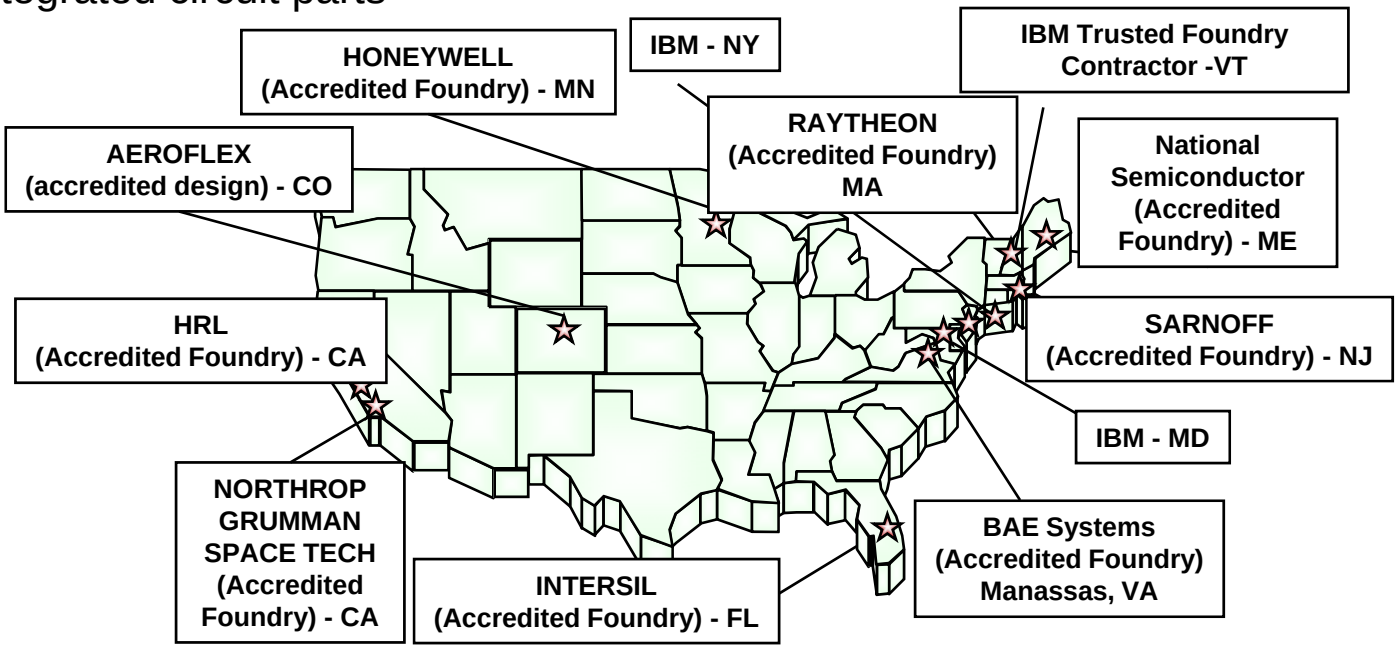
- SAWG Definition: System Assurance is *the justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle.*

  This ideal of no exploitable vulnerabilities is usually unachievable in practice, so programs must perform risk management to reduce the probability and impact of vulnerabilities to acceptable levels.

- This confidence is achieved by System Assurance Activities, which include a planned, systematic set of multi-disciplinary activities to achieve the acceptable measures of system assurance and manage the risk of exploitable vulnerabilities.

Trusted Access Program Office

- Integrated circuits in critical/essential systems need to be procured from trusted sources in order to avoid counterfeit, tampered, sabotaged or suborned parts
- Trusted Foundry Program executed jointly with NSA accredits semiconductor technology providers to serve as “trusted Foundries” and trusted suppliers.
  - Provides NSA with the trusted state-of-the-art microelectronics manufacturing
  - Provides DoD and its contractors with a cadre of trusted suppliers that will meet the needs of their mission critical/mission essential systems for trusted integrated circuit parts



CAS Program Objectives

Provide expert guidance on tools, techniques, and processes for software assurance measurement

- Bridge the gap between research and evaluation capabilities
- Form and lead a DoD assurance evaluation community to share best practices

Provide expert guidance on assured software implementation standards and practices

- Identify and mitigate “root causes” of vulnerabilities
- Drive the definition of “Quality” in DoD acquisitions and influence COTS development

Enable informed risk management in DoD acquisitions and software engineering by enhancing measurement capabilities, and also on secure coding principles and practices to make software worth measuring.

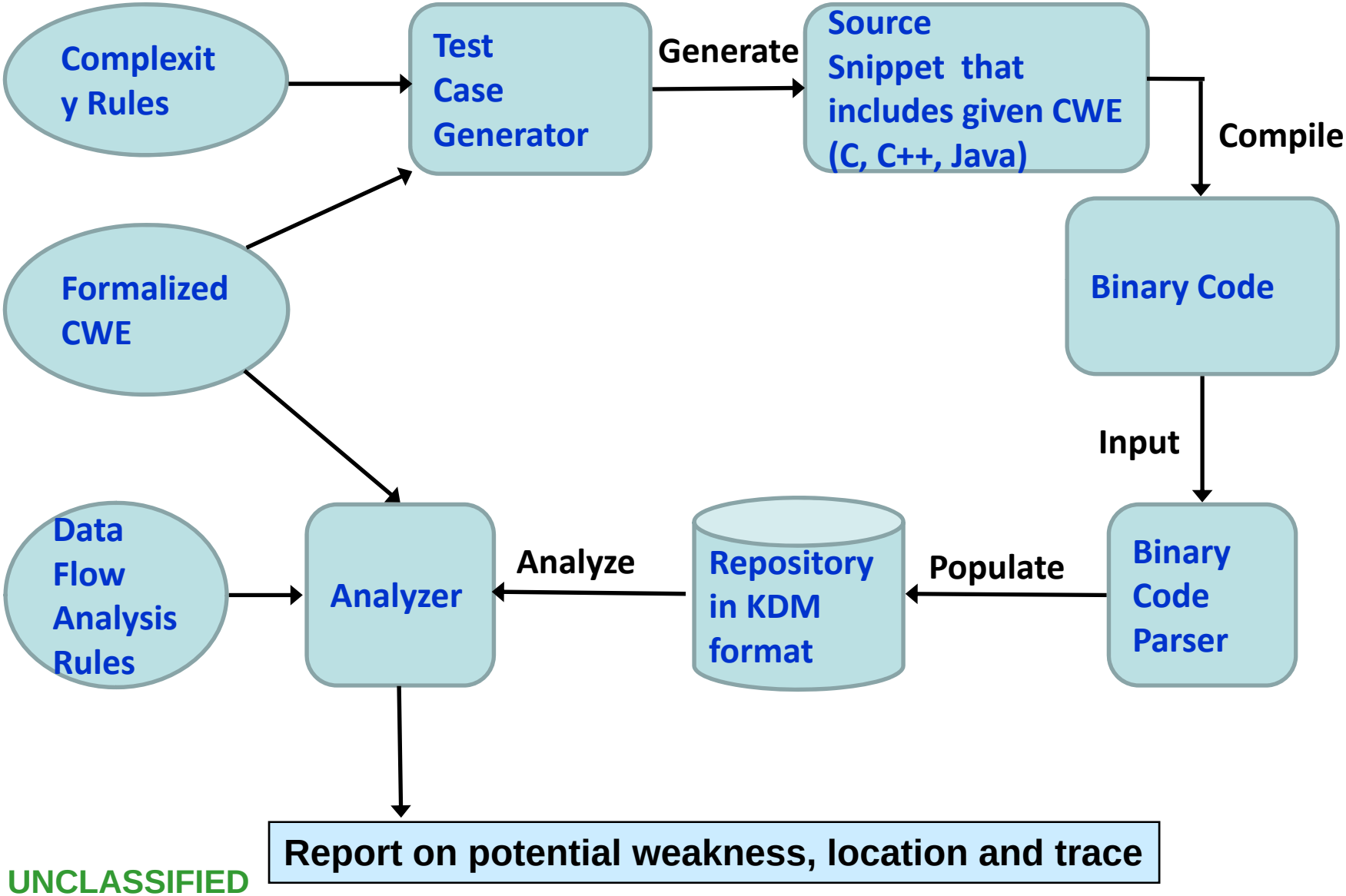
CAS Achievements

- Software Assurance Evaluation Methodology for C/C++ Source Code
  - Successful pilot evaluation of 4M SLOC
- Static Source Code Analysis Tools Evaluation Framework
  - Completed proof of concept evaluation of five leading commercial tools
- Works in Progress (FY08-FY09)
  - Updated Static Analysis Test Suite and Tool Evaluations for C/C++/Java
  - Development of binary executable analysis tools and techniques
  - Acquisition Security Risk Assessment Tool
  - Software Assurance Evaluation Survey and Best Practices Report

CWE Formalization and Analysis Proof of Concept

- Common Weakness Enumeration (CWE)
  - Currently uses informal definitions that are subject to varied interpretations
- Pilot investment by DOD and NSA to demonstrate the value of formalization to drive
  - Software Assurance analysis
  - Compliance checking
  - Generation of test cases
  - Generation of virtual patches
  - Generation of penetration and exploit tests
- Leveraging
  - OMG standards for formalization
    - Knowledge Discovery Metamodel (KDM)
    - Semantics of Business Vocabulary and Business Rules (SBVR)
  - NIST/DHS Test Case Generator
  - COTS analysis tools

Proof of Concept

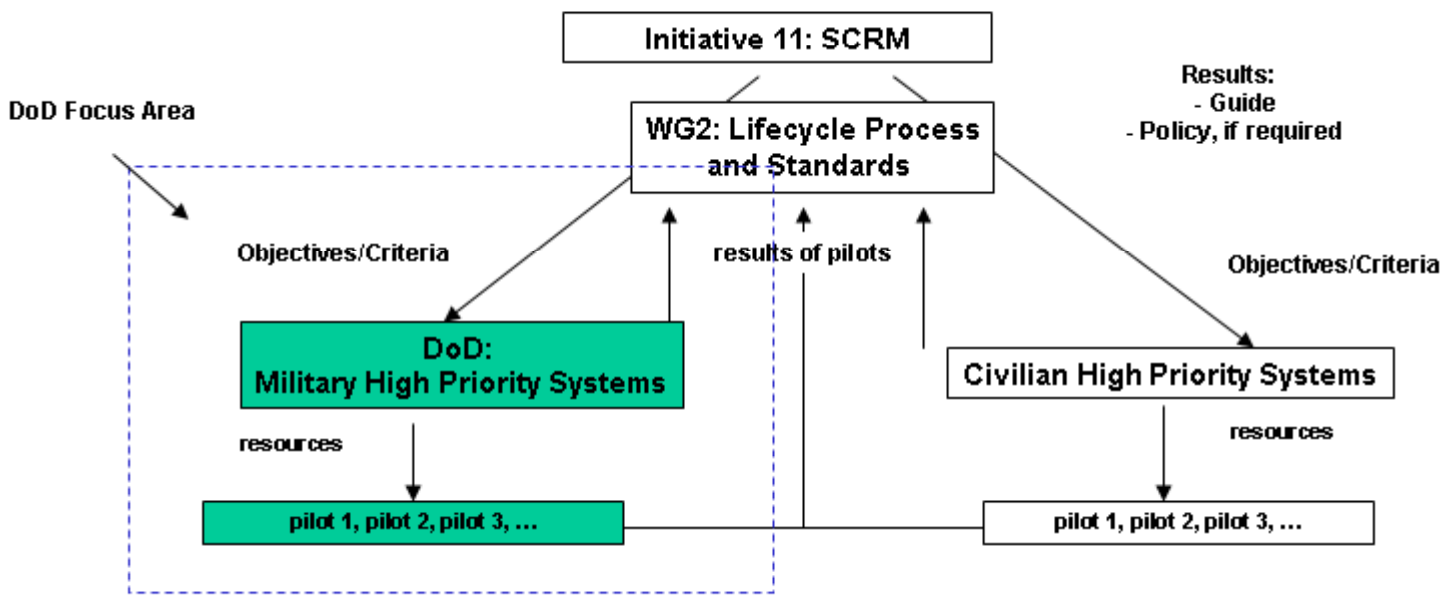


Benefits of Approach

- Clear separation of components
  - Security Properties
  - Software Engineering Constructs
    - Code constructs (CC)
    - Data-driven semantic analysis (e.g. DFA)
- Use of Standards
  - Interchangeable parts
  - Each component could come from different supplier
  - Each component can be addressed by experts in that domain
  - Components can be used for multiple disciplines
- End result of investment
  - Test Code Generator that automatically generates a very large set of code samples for use in testing and evaluating analysis tools
  - Demonstration that code (source or binary) can be analyzed against formalized CWEs

Next Steps in DoD

- Build on DODI 5200.39 by implementing SCRM in DoD
- Establish DoD Supply Chain Risk Assessment Capability
- Incrementally roll out SCRM through DoD Pilot programs
- Institutionalize SCRM within the Department through:
  - Procurement and acquisition policy
  - Systems Assurance Engineering
  - SW Assurance, HW Assurance (TAPO)
  - R&D



Expanding DoD Industry Partnership

- Acquisition Cyber Security is a long term interest for DoD
  - Fully anticipating Cyber Security will be a ongoing priority for the new administration
- Protecting DoD information wherever it resides
  - Secure networks, applications and systems
  - Preventing introduction of counterfeit components
- Managed consumption of COTS technologies and products
  - Enhanced Systems Engineering to identify and fortify critical components which implement or affect key functionality allowing incorporation of standard COTS for generic functions with appropriate isolation and separation
  - Industry outreach to explore industry thoughts for commercially reasonable assurance for globally sourced products

Questions?