

# Lessons Learned from the DHS/DoD Software Assurance Forum



## *Processes and Practices*

*Presented by  
Paul R. Croll*

*Chair, WG1, Processes & Practices  
Chair, IEEE CS Technical Council on  
Software Engineering*

*Chair, IEEE Software and Systems  
Engineering Standards Committee*

*Convener, ISO/IEC JTC1/SC7 WG9,  
System and Software Integrity*

Computer Sciences  
Corporation  
pcroll@csc.com

# Outline

- Why Now?
- Issues, Observations, Recommendations  
From The First Software Assurance Forum
- Requirements, Practice, Adoption,  
Knowledge Sharing
- Standards
- Practice Guidance
- Next Meetings

# Why Now?

- We're at a turning point, where the need for more assurance is becoming more pronounced.
- Vulnerability free is what we are looking for – where a vulnerability is defined in the eyes of the beholder.
- We want software that behaves as it was designed
- In the global market place, this may be a new discriminator for American industry to latch onto – in an international environment, this discriminator may give U.S. industry an edge.

# Software Assurance Forum: Working Group 1 Processes And Practices

## *Issues, Observations, And Recommendations from the First Software Assurance Forum*

# Issues and Observations Related to Processes and Practices

- Current development and acquisition processes inadequately address software risks and threats, and software-enabled functions.
- Acquisition organizations have a due-diligence responsibility to determine the capabilities of potential suppliers to deliver secure software.
- Current software development practices produce software that is riddled with defects, and some of those defects can lead to security vulnerabilities.
- 91% of defense acquisitions had performance issues attributable to the inability of the program team to specify, design, integrate, and implement processes that adequately support the needs of the program.
- Custom and COTS software will need to be treated differently.
  - The impact of open source software is not yet well understood.

*Source: Interim Report – SOFTWARE ASSURANCE: Mitigating Software Risks in the Department of Defense (DoD) Information Technology (IT) and National Security Systems (NSS)*

# Short-Term Recommendations

*To capitalize on the use of processes and practices that contribute to the delivery of safe and secure software-intensive systems and software-reliant networks, the DoD can take near term actions to influence software acquisition, development, and support, including:*

- *Enable the establishment of requisite infrastructure for software assurance.*
- *Ensure software assurance requirements are satisfied.*
- *Ensure activities and products will be managed to achieve software assurance requirements and objectives.*

*For suppliers:*

- *The time is right for widespread adoption of static assurance tools.*
- *There are several Capability Maturity Models and process framework standards that could be used to guide process improvement and provide criteria to evaluate process capabilities.*

Source: Interim Report – SOFTWARE ASSURANCE: Mitigating Software Risks in the Department of Defense (DoD) Information Technology (IT) and National Security Systems (NSS)

# Mid-Term Recommendations

*To ensure that future software processes and practices will be used to consistently produce secure products, DoD should sponsor the measurement and evaluation of software development processes. Moreover, DoD and DHS should co-sponsor accreditation requirements for information assurance, computer science and software engineering in universities and colleges.*

Source: Interim Report – SOFTWARE ASSURANCE: Mitigating Software Risks in the Department of Defense (DoD) Information Technology (IT) and National Security Systems (NSS)

# Far-Term Recommendations

*To prepare for the future, to ensure that software processes and practices will consistently produce secure products, DoD should sponsor research methods for verifying security in software-intensive systems and software-reliant networks. Moreover, DoD should sponsor research focused on ensuring systems and networks can operate in spite of software vulnerabilities being targeted for exploitation.*

Source: Interim Report – SOFTWARE ASSURANCE: Mitigating Software Risks in the Department of Defense (DoD) Information Technology (IT) and National Security Systems (NSS)

# Software Assurance Forum: Working Group 1 Processes And Practices

*Requirements, Practice,  
Adoption, Knowledge Sharing*

# Assurance Requirements Issues and Observations

- What does software assurance mean?
  - What the missing piece of requirement – lack of understanding with end customer – hence requirements don't get generated. You can't choose the right processes if you don't know what the right requirements are.
- You don't want to have unknown, non-specified functionality in software.
- The boundary between Information Assurance and Software Assurance is not clear and should be defined more carefully.
- What are our assurance requirements?
  - Want software to behave deterministically.
  - Software developed in a way that withstands malicious use.
  - Reliable in the face of intentional faults.
  - Consider the warfighter.
  - What else?

# NIST's Definition

Grounds for confidence that the . . . four security objectives (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. “Adequately met” includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass.

*NIST Special Publication 800-33, Underlying Technical Models for Information Technology Security, December 2001*

# NASA's Definition



Software assurance is the planned and systematic set of activities that ensures that software processes and products conform to requirements, standards, and procedures. "Processes" include all of the activities involved in designing, developing, enhancing, and maintaining software; "products" include the software, associated data, its documentation, and all supporting and reporting paperwork.

*NASA SMAP-GB-A201, "Software Assurance Guidebook"*

*NASA-STD-2201-93, "Software Assurance Standard"*

# ISO/IEC JTC1/SC7/WG9 Terms of Reference

System and software assurance addresses management of risk and assurance of safety, security, and dependability within the context of system and software life cycles.

*ISO/IEC JTC1/SCT Working Group 9, System and Software Assurance*

# Assurance Is A Life Cycle Issue

**“ . . . The key difference between secure software and insecure software is the nature of the development process used to specify, design, code, integrate, install, and maintain that software. The development organization that adopts a ‘security-enhanced’ software development life cycle process will be adopting a set of practices that will initially reduce the number of exploitable defects, or vulnerabilities, in their implemented software, and over time will decrease the likelihood that such vulnerabilities will be introduced into their software in the first place.”**

*Security in the Software Lifecycle: Making Application Development Processes – and the Software Produced by Them – More Secure (Draft v0.8), Department of Homeland Security, January 9, 2006*

# Assurance Practice Issues and Observations

- We need to do a gap analysis, with respect to assurance concerns, on what we know are good software engineering practices.
  - Good software engineering leads to good software assurance
  - Doing good software engineering solves 90% of the assurance problems
  - There is still a 10% problem, no matter how much good engineering you do
    - What does that extra 10% look like?
    - Vulnerabilities can be taken for good and for evil.
    - Remaining 10% may not be manageable by good software engineering
- We cannot establish a practice without understanding the software assurance objectives of the Department
  - Need to articulate the Department's SA objectives and requirements so we have a framework for creating practices

# Best Practices Discussion

- When developing best practices, what is meant by the term “best practices” and who is the audience for the best practices? What is the level that the practice should address – the process level, the technical level?
- It would be helpful to develop a matrix, to be filled in via email, to determine what roles/effect the practices would have on the owners, planners, designers, builders, certifiers
- Where is the line between a “standard” and a “best practice”?
- Do engineers who are hired to develop software today have experience in developing secure code as part of their educational background or is that something that is learned “on the job”?
- Metrics must be developed to measure the success of a practice, not only for avoiding detrimental practices, but also to be used in the development of a business case and as a marketing tool.

# Assurance Adoption Issues and Observations

- We can discuss what we need in software security, but vendors won't do it until we make it worth their while.
  - Need to factor it into the acquisition process
  - How do we incentivize the industry to go out and build secure software?
- Efficiencies and bottom line concerns often do not involve software assurance.
  - No way to put the time and effort in to deliver secure software.
  - If government is not willing to put it in as a hard requirements – you won't get it.
- A study of patch management costs vs. costs of developing secure software might provide some ammunition for doing it right the first time.
- COTS is different – low price comes essentially at an assurance cost
  - Need to understand what you're actually getting for the price, for commodity software
- What are the adverse consequence for vendors when they don't meet security requirements?
  - When we use commercial products we sign a waiver assuming all risk and liability

# Knowledge Sharing Issues and Observations

- Where do we put all this practice information so it's accessible to community?
  - Need a central area where information is available to entire community
  - Collaboration areas have been set up on the US-CERT Portal
    - By invitation to WG members: <https://us-cert.esportals.net/>
    - Build Security In website: <https://buildsecurityin.us-cert.gov/portal/>
- We must undertake outreach efforts for this working group
  - We want to have a place where both government and industry can come together to discuss issues and make recommendations

# Expectations For The Future

## *Where do we go from here?*

- What type of tools could the buying community use that could be provided by the vendor community?
- For organizations that have implemented best practices, how did they do it, what were the choices/trade-offs that were made?
- What is being done to help the customer ask the right questions?
- Development of a methodology and security criteria that could be used as part of “purchase specifications”.
- Development of 5-10 pages of criteria/guidance that could be used to make it easier for buyers to purchase more secure software.
- Development of a developer’s guide which speaks to the security evaluation of components.
- Development of a “roadmap” to lay out the steps necessary to become “software assured” and to allow stakeholders to “know what they don’t know.”
- Discussion/information provided on foreign influence control issues, specifically, what questions should critical infrastructure operators know to ask.

# Software Assurance Forum: Working Group 1 Processes And Practices

## *Standards*

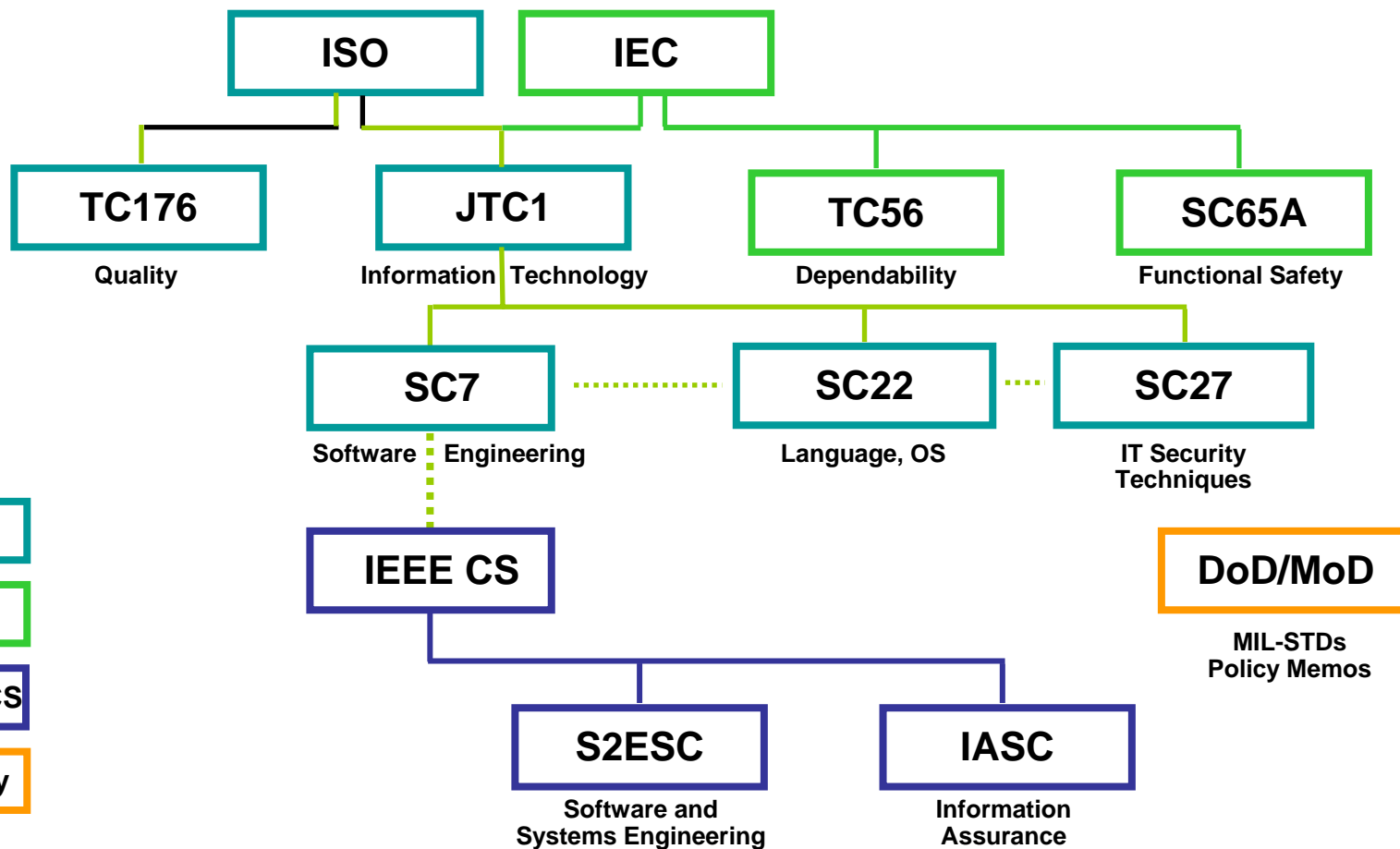
# Standards Issues

- Do they focus on developing processes and paradigms for information assurance controls, or do they reach down into the basics of the software development process itself?
- Should we be creating extensions to existing standards to address software assurance aspects, to ensure software assurance standards aren't separate from other standards?
- What do we have now, in terms of standards, that we can piece together, and what holes do we have to fill?

# Standards Observations

- We have a lot of standards – but not they're not necessarily harmonized.
- There needs to be a set of “assurance” standards for industry to follow.
  - Standards and best practices web sites should have a matrix that directs you to look at certain standards.
  - Two options – insert what software assurance means into existing standards or define a discrete set of standards.
- Standards can be viewed as a risk management activity, but they must be very explicit about addressing threats for both safety and security.
- Assurance concerns need to become part of the software lifecycle process.
  - Focus on establishing what are the assurance characteristics that we are looking for – better defining what software assurance is – so that we can select standards and define processes to address them.
- Standards will be ignored unless they're put on contract. If that's done then conformance is a matter of quality assurance.

# Some Standards Organizations Supporting Assurance



# Safety and Security Standards

## Dependability

**IEC 61713**  
 Software dependability through the software life-cycle processes

**IEC 61508**  
 Functional Safety

**IEEE 1228**  
 SW safety plans

## Military Standards

**MIL-STD-882D**  
 Standard Practice for System Safety

**DEF STAN 00-56**  
 Safety Management Requirements for Defence Systems

**IEC**

**IEEE CS**

**Military**

**RTCA**

**Safety**

## Sector-Specific Standards

**IEC 60880**  
 SW in nuclear power safety systems

**DO 178B**  
 SW considerations in airborne equipment certification

**ISO/IEC 15408**  
 Common Criteria for IT Security Evaluation

**ISO/IEC 10181**  
 Security frameworks for open systems

**ISO/IEC 9796**  
 Digital Security Schemes

**IEEE P1700**  
 Security Architecture for Certification and Accreditation of Information

**Security**

**ISO/IEC 15443**  
 Framework for IT Security Assurance

**ISO/IEC 21827**  
 Systems Security Engineering CMM

**IEEE P1619**  
 Standard Architecture for Encrypted Shared Storage Media

**ISO**

**IEEE CS**

**ISO/IEC 17799**  
 Code of Practice for Information Security Management

**ISO/IEC 27001**  
 Information Security Management System (ISMS) Requirements

**P1667**  
 Standard Protocol for Authentication in Host Attachments of Transient Storage Devices

**IEEE P2200**  
 Baseline Operating System Security

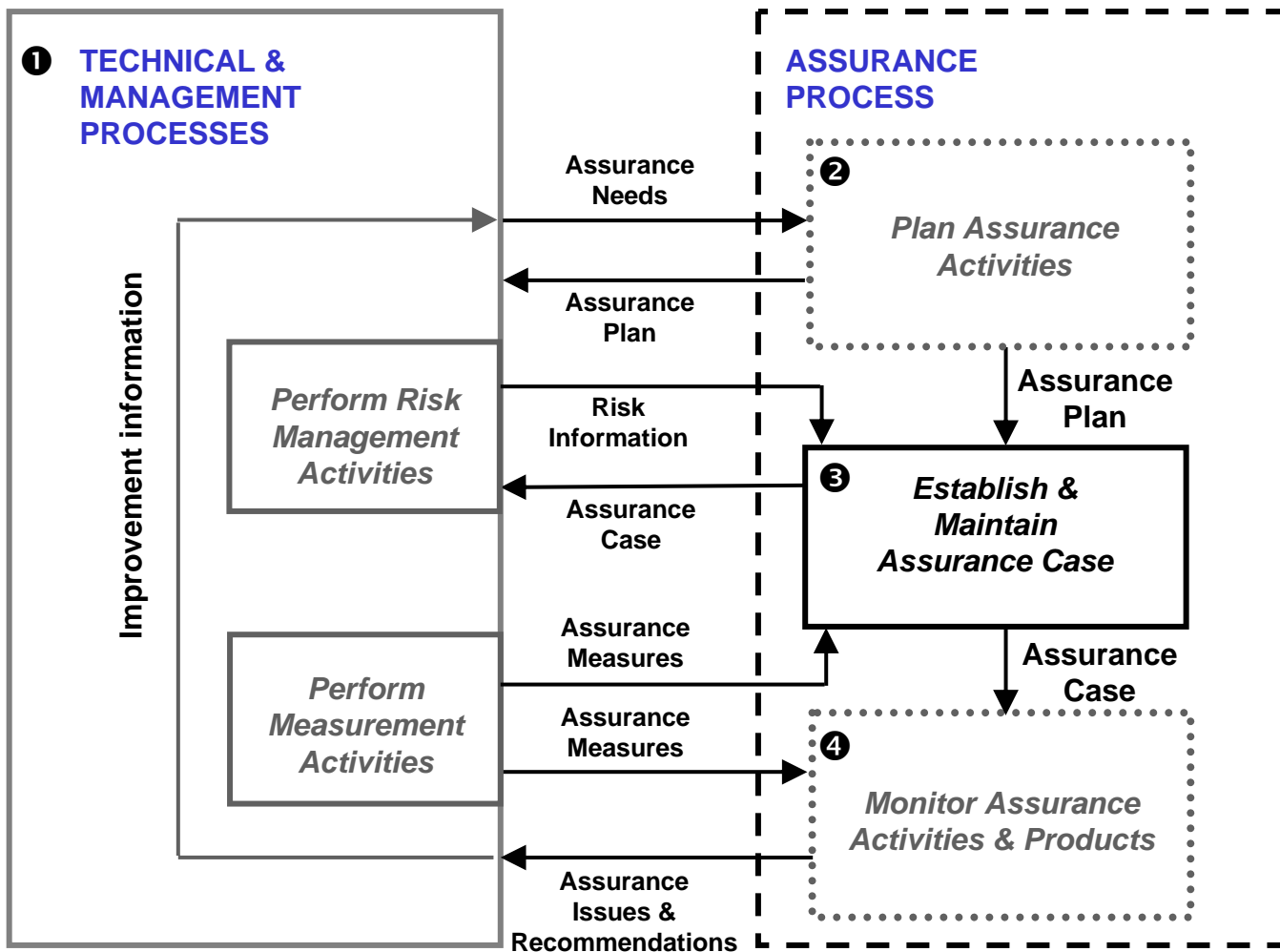
**IEEE CS Under Development**



# ISO/IEC 15026 – System and Software Assurance

- Describes an assurance process that provides sufficient evidence that a system satisfies its critical requirements throughout the life cycle of a product or service
- Consists of the following activities:
  - Plan assurance activities
  - Establish and maintain the assurance case
  - Monitor assurance activities and products

# ISO/IEC 15026 – Context Diagram



Source:  
 ISO/IEC 15026,  
 System and  
 Software  
 Assurance,  
 Working Draft 4

# Planning Assurance Activities

- The assurance plan shall ***establish the objectives, activities, resources, and responsibilities*** for safety, security, and dependability ***throughout the product or service life cycle***, including, as appropriate, development, deployment, operation, and disposal.
- An assurance plan shall address:
  - Scope of the work and work products to be developed
  - Description of the product or service life cycle
  - Goals and objectives to be measured
  - Cost, schedule, and resource estimates
  - Safety, security, and dependability analysis activities
  - Risk assessment procedures and analysis techniques
  - Risk tracking and resolution procedures, including mitigation, review, and acceptance procedures
  - Plans for supporting activities such as product and service evaluations, configuration management, quality management, etc.
  - Roles and responsibilities for identified activities
  - Stakeholder involvement

# Establishing And Maintaining The Assurance Case

- An assurance case shall be established, consisting of a ***set of structured assurance claims, supported by evidence and reasoning***, that demonstrates how assurance needs have been satisfied. The assurance case shall show how compliance with assurance objectives have been met and provides an ***argument for the safety and security of the product or service***. The arguments and supporting evidence shall be built, collected, and maintained ***throughout the life cycle*** and are typically derived from multiple sources. These sources may include artifacts generated from several other application practices, as determined in the information management strategy and requirements.

# The Assurance Case – Structure and Attributes

Part 1

A coherent argument  
for the safety and  
security of the product  
or service

Part 2

A set of supporting  
evidence

...

...

...

## *Attributes*

- Clear
- Consistent
- Complete
- Comprehensible  
(to all relevant  
stakeholders)
- Bounded
- Defensible
- Should cover all  
stages of the life  
cycle

# The Assurance Argument

- A high level summary of the claim(s)
- Justification that the product or service is acceptably safe, secure, or dependable
- Rationale for claiming a specified level of safety and security
- Citation of relevant standards and regulatory requirements
- Identification of the configuration baseline
- Identified hazards and threats and the residual risk of each hazard and threat
- Operational and support assumptions

# Monitoring Assurance Activities And Products

- Assurance activities shall be monitored ***throughout the product or service life cycle.*** Proposed changes to policies, procedures, plans, products, and services shall be subjected to ***assurance impact analyses.*** Issues and recommendations resulting from monitoring activities shall be ***reported to relevant stakeholders.***
- Review and audit of ***configuration management procedures and activities*** should be done to prevent accidental or unauthorized modifications of controlled products.

# ISO SC27 IT Security Standards

## ■ Key Standards

- ISO/IEC 27000 series – Information Security Management System (ISMS)
- ISO/IEC 17799:2005 – Code of Practice for Information Security Management
- ISO/IEC 21827, System Security Engineering Capability Maturity Model (SSE CMM) revision
- ISO/IEC 15443, FRITSA
  - Part 1: A framework for IT security assurance
  - Part 2: Assurance methods
  - Part 3: Analysis of assurance methods
- ISO/IEC DTR 19791, Assessment of Operational Systems

## ■ SC27 looking at new topics

- Privacy
- Identify management
- Biometric protection and evaluation

# OMG Software Assurance Framework

## ■ Goal

- Achieve transparency of the product

## ■ Objective

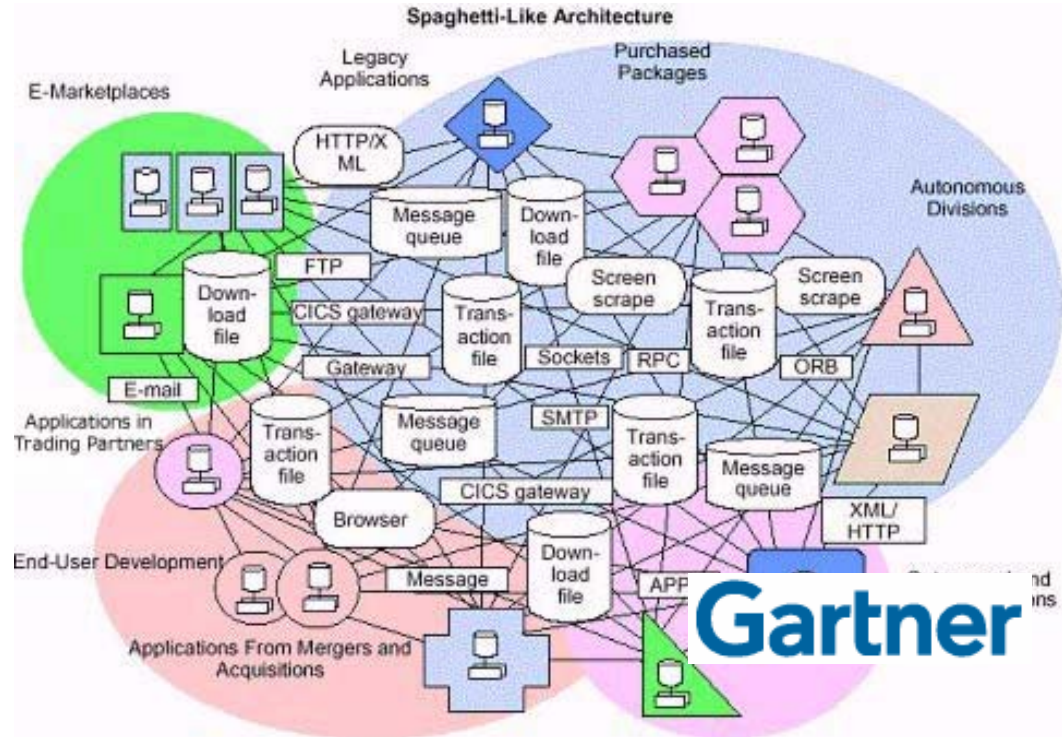
- Provide a standard for a collaborative framework to facilitate information exchange regarding claims, arguments, evidences, consequences, risks

## ■ Mechanism

- A layered Knowledge Discovery Model (KDM) to facilitate extraction of artifacts and relationships from source code
  - Focuses on the existing system and how one extracts artifacts to help validate product security

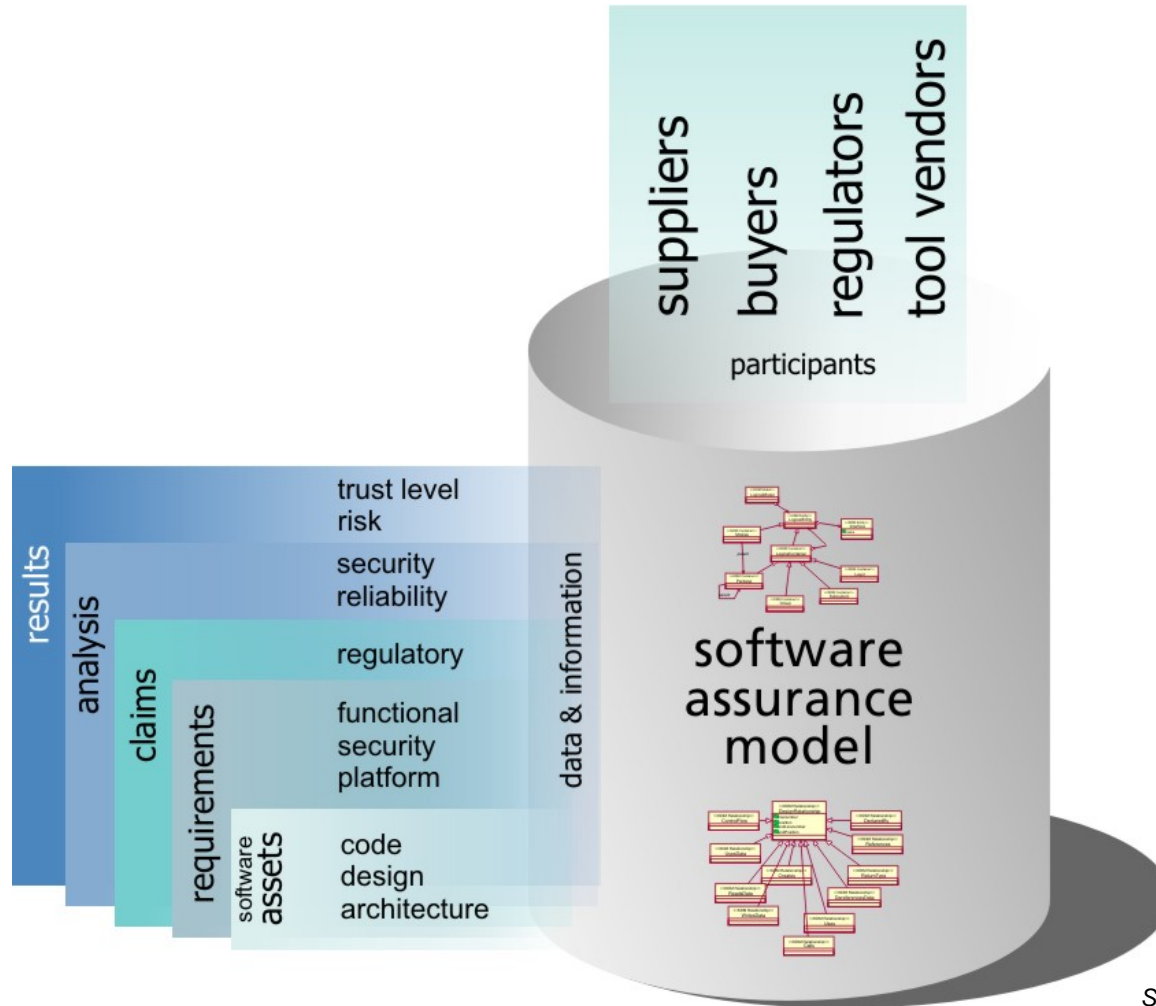
# The Knowledge Discovery Problem: Complexity, Multiple Technologies, Multiple Vendors

- Complexity
- COTS/GOTS/Reuse
- Existing software assets
- Hybridization
- Evolution
- Erosion of Knowledge
- Globalization
- Lack of Skills



***These factors make increasingly difficult to assess the properties of software systems, such as quality, reliability, performance, robustness, and trustworthiness***

# Focus is on Coordinated Model Strategy



Source: Djenana Campara  
CTO, Klocwork Inc.  
OMG, Co-Chair: ADMTF & SwA

# Software Assurance Forum: Working Group 1 Processes And Practices

## *Practice Guidance*

# DISA Security Technical Implementation Guides (STIGs)

- STIGs can help, as compliance checklists to promote Software Assurance.
- STIGs are:
  - A Compendium of DOD Policies, Security Regulations and Best Practices for Securing an Operating System or Application Software
  - A Guide for Information Security
  - Use is Mandated in DISA by DISA Instruction 630-230-31
  - Endorsed by CJCSI 6510.01 and DODD 8500.1 and DODI 8500.2
- STIGs focus on:
  - Intrusion Avoidance
  - Intrusion Detection
  - Response and Recovery
  - Security Implementation Guidance

# Current STIGs

## ■ NETWORK/PERIMETER

IP WAN	Enclave	Network Infrastructure
Wireless	DNS	Secure Remote Computing

## ■ OPERATING SYSTEM

OS 390 (MVS)	VM	LPAR
Unisys	Tandem	UNIX
Win NT (NSA)	Win 2K (NSA)	Win NT/2K/XP Addendum
Win XP (NSA)	Win2003 (MS)	Macintosh

## ■ APPLICATION

Database	Web Server	VOIP
Desktop Applications	DSN	Biometric
DATMS		

## ■ USER

Security Handbook

## ■ AVAILABLE AT THE FOLLOWING WEB SITE

<http://iase.disa.mil>



Source: Terry Sherald, CISSP  
DISA Field Security Operations

# How Can They Be Used?

- Application Developers Guidance
- SA Implementation Guidance
- Self-Assessments of Security Posture
- Certification / Accreditation Tool
- Information Assurance Review Process

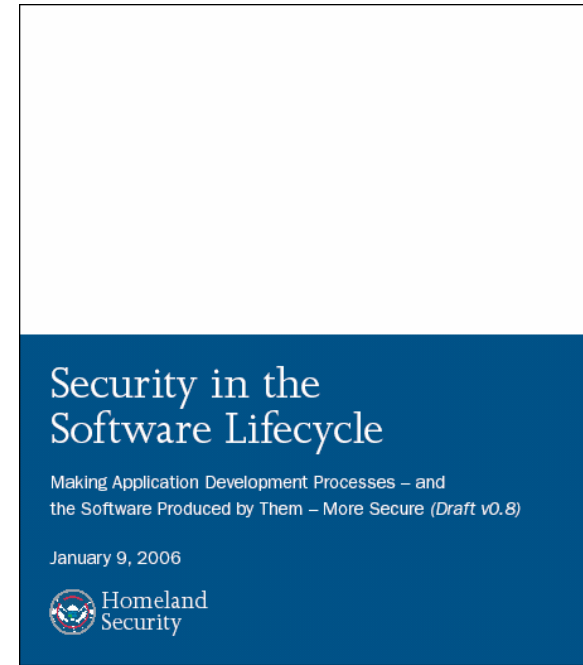


Source: Terry Sherald, CISSP  
DISA Field Security Operations

# Security in the Software Lifecycle

## *Making Application Development Processes – and the Software Produced by Them – More Secure*

- A resource to help developers and project managers produce secure software
- Describes motivations for secure software
- Presents software security definitions, concepts, and principles
- Introduces best practices for “sooner rather than later” adoption throughout the lifecycle
- Reports on “security-enhanced” lifecycle process models and development methodologies
- Presents security benefits and shortcomings of popular methodologies



- Of particular interest
  - *APPENDIX C: Common Attacks Against Web Applications And Web Services*
  - *APPENDIX G. In The Meantime: Practices To Adopt Sooner Rather Than Later*

# Secure Software Assurance

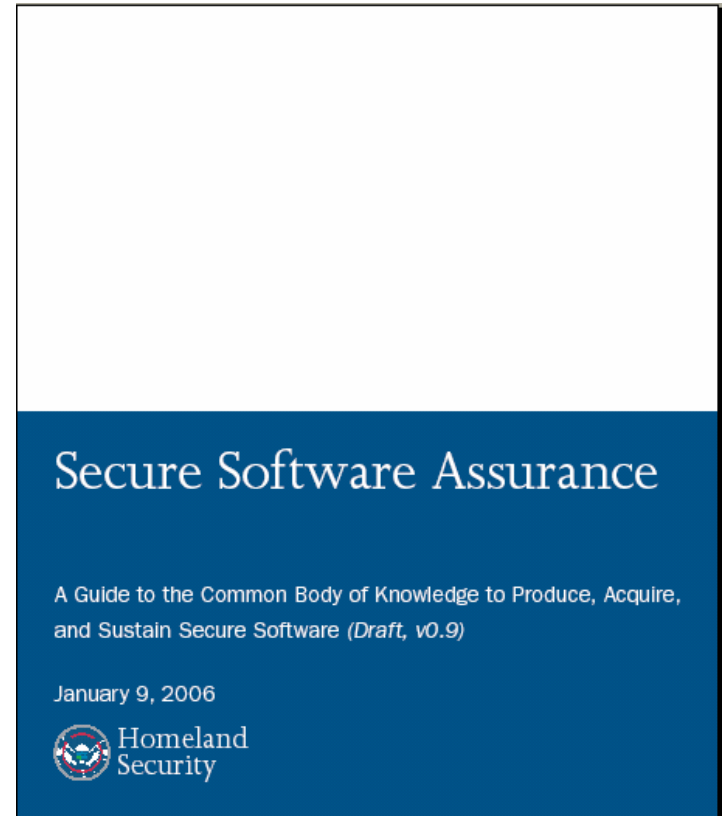
## *A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software*

### ■ Content

- identifies the “additional” knowledge needed for developing, sustaining, and acquiring secure software

### ■ Motivation

- What are the engineering activities or aspects of activities that are relevant to achieving secure software?
- What knowledge is needed to perform these activities or aspects?



# Joint Industry/DoD/DHS Efforts in System Assurance

- NDIA System Assurance Committee
  - Chartered by the NDIA Systems Engineering Division
  - Sponsor: Director, Systems Engineering, OUSD AT&L/DS
- DoD Engineering-in-Depth Approach to System Assurance
  - Fundamentally a systems engineering problem
    - Minimize the engineering impact to program-level cost, schedule and performance
    - Support development of the processes and procedures to mitigate software-attributable vulnerabilities
- Plan of Action: Identify Opportunities to Enhance Systems Engineering Guidance to Reflect System Assurance Practices
  - Establish membership from across all communities of interest
    - Traditional DoD industrial base
    - Commercial industry (component suppliers)
    - Non-defense industry system engineers/integrators
    - Capture current industry practices
  - Publish a System Assurance white paper
    - Definition of System Assurance Problem
    - Systems/Software engineering community goals
  - Develop a System Assurance Handbook
    - Supplementary information for the Defense Acquisition Guidebook
  - Develop a plan for leveraging relevant standards and identifying gaps
    - Engaging IEEE, ISO, OMG, AIA, GEIA

# Next Meetings

Please contact Cindy Gagliano at [Cindy.Gagliano@associates.dhs.gov](mailto:Cindy.Gagliano@associates.dhs.gov) with an indication of the Working Group Session(s) that you are planning to attend. The Working Groups will be held at Booz Allen Hamilton at 3811 N. Fairfax Drive, Suite 600 Arlington, VA 22203. Directions will be sent with the confirmation email.

	Tuesday, May 9th	Wednesday May 10th	Thursday, May 11th
Morning 8:30 - 11:30	Session 1: Technology WG	Plenary Session	Session 5: Acquisition WG
	Session 2: Measurement WG		Session 6: Business Case WG
Afternoon 1pm - 5pm	Session 1: Technology WG	Session 3: Processes & Practices WG	Session 5: Acquisition WG
	Session 2: Measurement WG	Session 4: Workforce Training WG	Session 6: Business Case WG

# For More Information . . .

Paul R. Croll  
Computer Sciences Corporation  
5166 Potomac Drive  
King George, VA 22485-5824

Phone: +1 540.644.6224  
Fax: +1 540.663.0276  
e-mail: [pcroll@csc.com](mailto:pcroll@csc.com)

