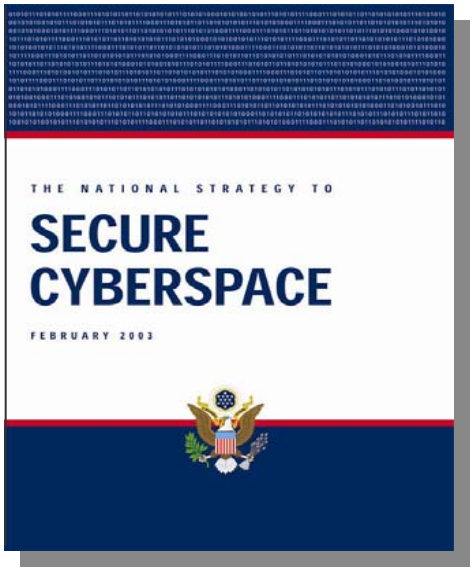
Software Assurance:

A Strategic Initiative of the U.S. Department of Homeland Security to Promote Integrity, Security, and Reliability in Software



An Enabling Role and a Broader Perspective for Measurement

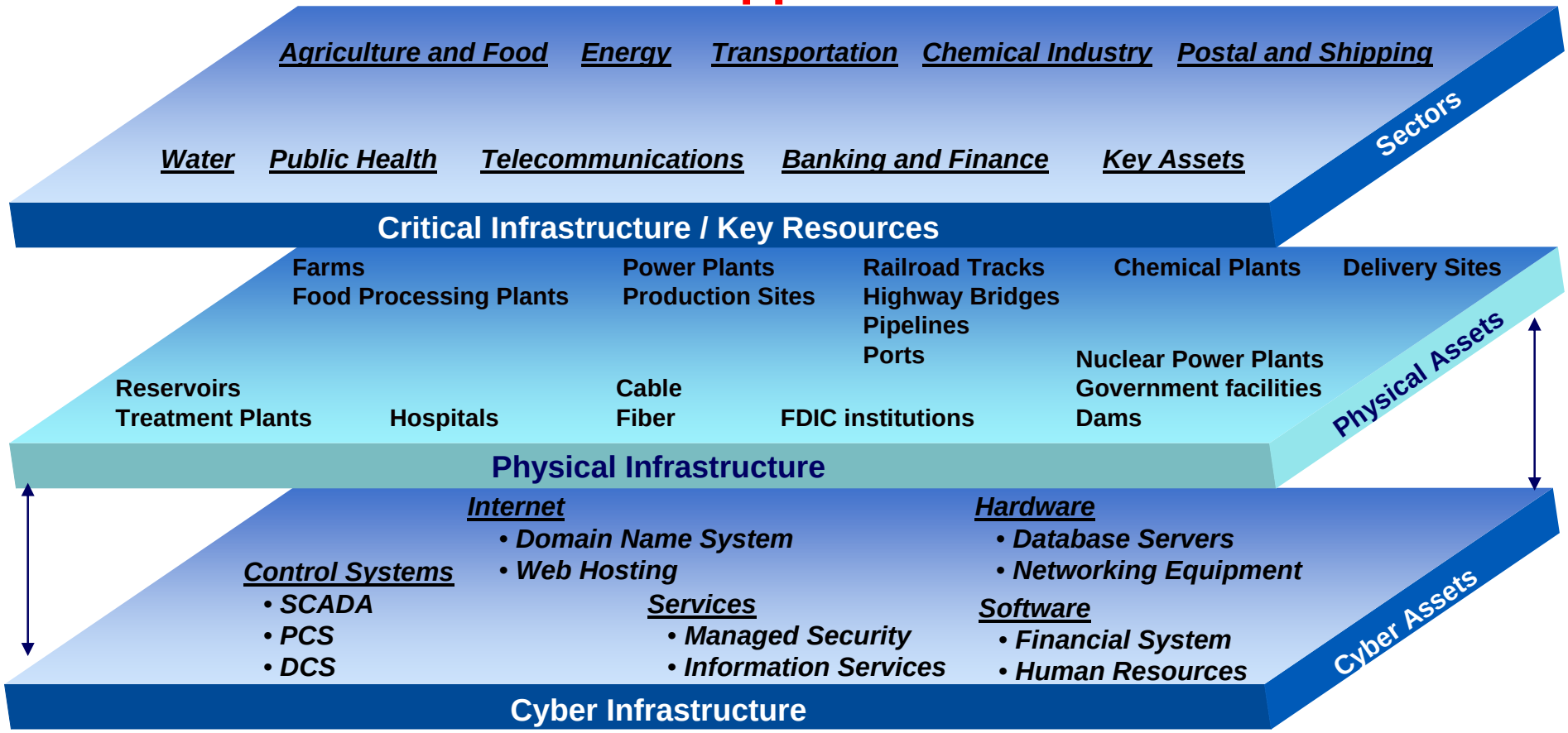
July 24, 2007

Homeland Security

Joe Jarzombek, PMP
Director for Software Assurance
National Cyber Security Division
US Department of Homeland Security
Nadya Bartol, CISSP, ISSPCS
Booz Allen Hamilton

Cyberspace & physical space are increasingly intertwined and software controlled or enabled

Need for secure software applications *



*** 90% of software attacks were aimed at application layer**
(Gartner & Symantec, June 2006)

Homeland Security

"In an era riddled with asymmetric cyber attacks, claims about system reliability, integrity and safety must also include provisions for built-in security of the enabling software."

Cyber-related Disruptions and the Economy

- 75% of hacks occurred at application level (Gartner 05)
  - 90% of software attacks were aimed at application layer (Gartner & Symantec, June 2006)
- Cyber disruptions lead to loss of:
  - Money and Time
  - Products, Sensitive information, Reputation
  - Life (through cascading effects on critical systems and infrastructure)
- Meta-trends:
  - Worms & viruses increasingly sophisticated
  - More variants of older, successful worms
  - New vulnerabilities have black market value; increasing "zero-day" exploits

- **$67.2 Billion a year is lost to cyber crime in the USA** (FBI 2005)
- **$50-200M in average shareholder losses** (CRS 2006)
- ***80%* of hack attacks emanate from outside of user enterprise** (2005 US-CERT-CSO E-crime Survey)
- **9 out of 10 businesses affected by cyber crime last year** (FBI 2005)

Business Losses and Damages

Love Bug: $15B in damages; 3.9M systems infected 2000	**Code Red:** $1.2B in damages; $740M for recovery efforts 2001	**Slammer:** $1B in damages 2002	**Blaster:** $50B in damages 2003	**My Doom:** $38B in damages 2004	**Zotob:** Damages TBD 2005

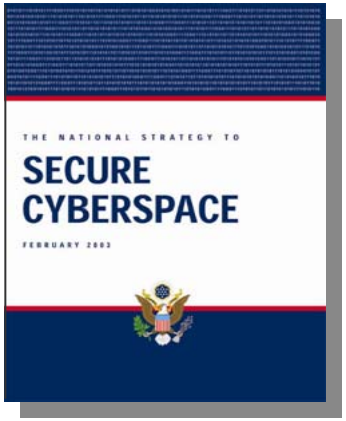
Homeland Security

Over $40 million in spyware damages – attacks now are "designed to silently steal data for profit or advantage without leaving behind the system damage that would be noticeable to the user."
(Congressional Testimony, HE &Commerce Telecomm/Internet Subcommittee, Sep 12, 2006)

DHS Software Assurance Program Overview

- Program based upon the National Strategy to Secure Cyberspace - Action/Recommendation 2-14:

  "DHS will facilitate a national public-private effort to promulgate best practices and methodologies that promote integrity, security, and reliability in software code development, including processes and procedures that diminish the possibilities of erroneous code, malicious code, or trap doors that could be introduced during development."



- DHS Program goals promote the security of software across the development, acquisition and implementation life cycle
- Software Assurance (SwA) program is scoped to address:
  - **Trustworthiness** - No exploitable vulnerabilities exist, either maliciously or unintentionally inserted
  - **Predictable Execution** - Justifiable confidence that software, when executed, functions as intended
  - **Conformance** - Planned and systematic set of multi-disciplinary activities that ensure software processes and products conform to requirements, standards/ procedures

Also See Wikipedia.org for Software Assurance

Homeland Security

CNSS Instruction No. 4009, "National Information Assurance Glossary," Revised 2006, defines Software Assurance as: "the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner".

DHS Software Assurance Program Structure *

- As part of the DHS risk mitigation effort, the SwA Program seeks to reduce software vulnerabilities, minimize exploitation, and address ways to improve the routine development of trustworthy software products and tools to analyze systems for hidden vulnerabilities.
- The SwA framework encourages the production, evaluation and acquisition of better quality and more secure software; leverages resources to target the following four areas:
  - **People** – education and training for developers and users
  - **Processes** – sound practices, standards, and practical guidelines for the development of secure software
  - **Technology** – diagnostic tools, cyber security R&D and measurement
  - **Acquisition** – due-diligence questionnaires, contract templates and guidelines for acquisition management and outsourcing

Homeland Security

* July 28, 2006 statement of George Foresman, DHS UnderSecretary for Preparedness, before the U.S. Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Federal Financial Management, Government Information, and International Security

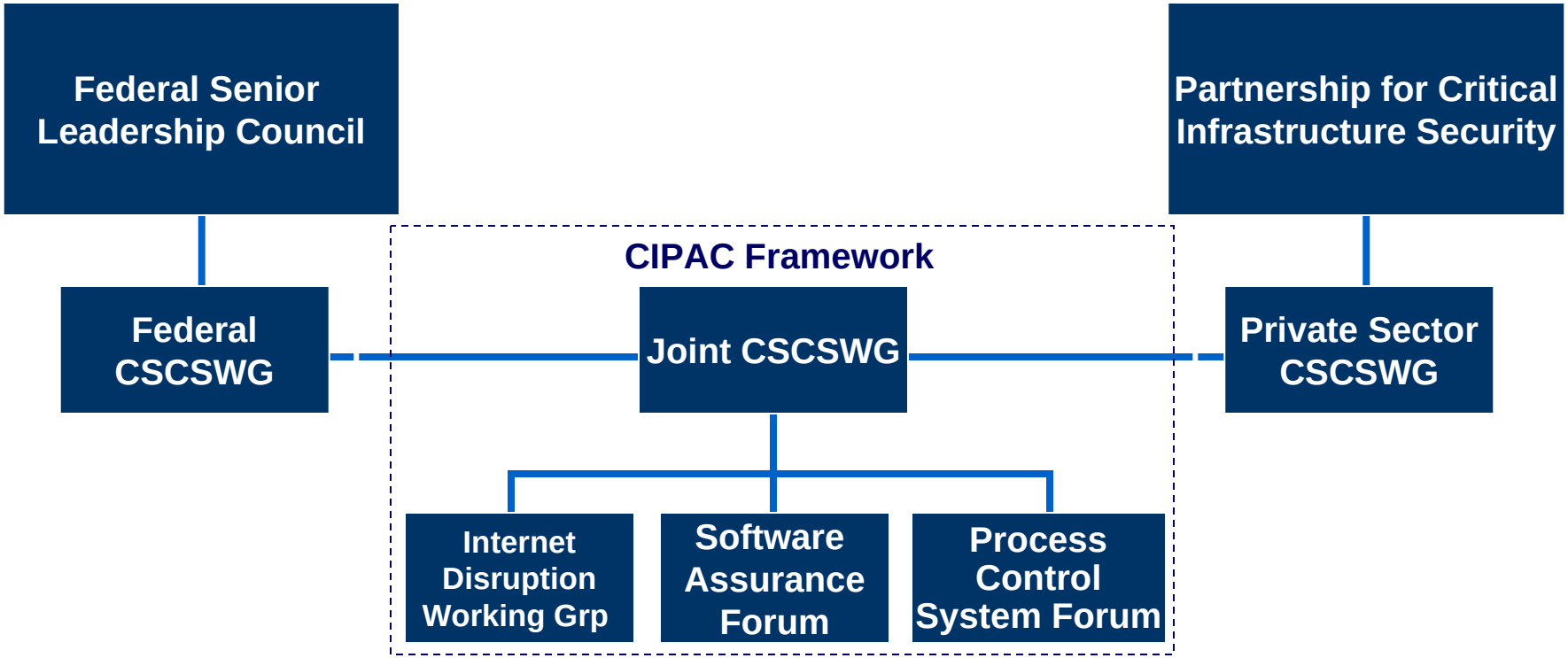
DHS Software Assurance (SwA) Outreach

- Co-sponsor bi-monthly SwA WG sessions and semi-annual Software Assurance Forum for government, academia, and industry to facilitate the ongoing collaboration -- next 2-3 Oct 2007
- Co-sponsor SwA issues of CROSSTALK (since Oct 05); provide SwA articles in other journals to "spread the word" to relevant stakeholders
  - March 2007 issue on "Software Security"
  - May 2007 issue on "Software Acquisition"
  - Sep 2007 issue on "Service Oriented Architecture"
- Provide free SwA resources via "BuildSecurityIn" portal to promote relevant methodologies
- Launch http://us-cert.gov/SwA for Software Assurance Community of Practice (Summer 07)
- Provide DHS Speakers Bureau speakers
- Support efforts of consortiums and professional societies in promoting SwA

INPUT TargetVIEW

Homeland Security

Collaborative Model with Public and Private Organizations



Cross-Sector Cyber Security Working Group (CSCSWG) established under auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC) provides legal framework for participation.

Homeland Security

DHS handles all necessary Secretariat and administrative processes and procedures necessary to comply with CIPAC policies.

Bi-Monthly Working Groups & Semi-Annual SwA Forum:

Next WG sessions held 4-6 Dec 2007 – Next SwA Forum 2-3 Oct 2007

Typical Format	Tuesday	Wed	Thursday
Morning 9:00am - 11:30am	**Session 1:** *Technology, Tools & Product Evaluation Working Group*	**Plenary Session**	**Session 6:** *Processes & Practices Working Group on "Argument/Case"*
	Session 2: *Business Case Working Group*		**Joint Session 8:** *Measurement WG with another SwA WG*
Afternoon 1pm - 5pm	**Session 1:** *Technology, Tools & Product Evaluation Working Group*	**Session 4:** *Malware Working Group*	**Session 6:** *Processes & Practices Working Group on "Argument/Case"*
	Session 3: *Workforce Education & Training Working Group*	**Session 5:** *Acquisition Working Group*	**Session 7:** *Measurement Working Group*

Presentations from previous SwA WGs and Forums are on US-CERT Portal (https://us-cert.esportals.net/) under the appropriate Working Group in the Library folder. Access to WG folder is restricted to those who have participated in the WG. Contact DHS NCSD if you do not yet have access to the appropriate folders.

Software Assurance (SwA) Forum and Working Groups …

… encourage the production, evaluation and acquisition of better quality and more secure software through targeting

People	Processes	Technology	Acquisition
Developers and users education & training	Sound practices, standards, & practical guidelines for secure software development	Security test criteria, diagnostic tools, common enumerations, SwA R&D, and SwA measurement	Software security improvements through due-diligence questions, specs and guidelines for acquisitions/ outsourcing

Products and Contributions

Build Security In - https://buildsecurityin.us-cert.gov and SwA community portal – http://.us-cert.gov/SwA

SwA Common Body of Knowledge (CBK) & Glossary
SwA Developers' Guide on Security-Enhancing SDLC
Systems Assurance Guide (via DoD and NDIA)

SwA-related standards – ISO/IEC JTC1 SC7/27/22, IEEE, OMG and CMM-based Assurance extensions

Software Security Assurance State of the Art Report

Practical Measurement Guidance for SwA/InfoSec

SwA Metrics & Tool Evaluation (with NIST) and SwA Ecosystem (with DoD, NSA, NIST & OMG) and NIST Special Pub 500 Series on SwA Tools

Common Weakness Enumeration (CWE) dictionary
Common Attack Pattern Enumeration (CAPEC)
Common Malware Enumeration (with ASC)

SwA in Acquisition: Mitigating Risks to Enterprise

Homeland Security

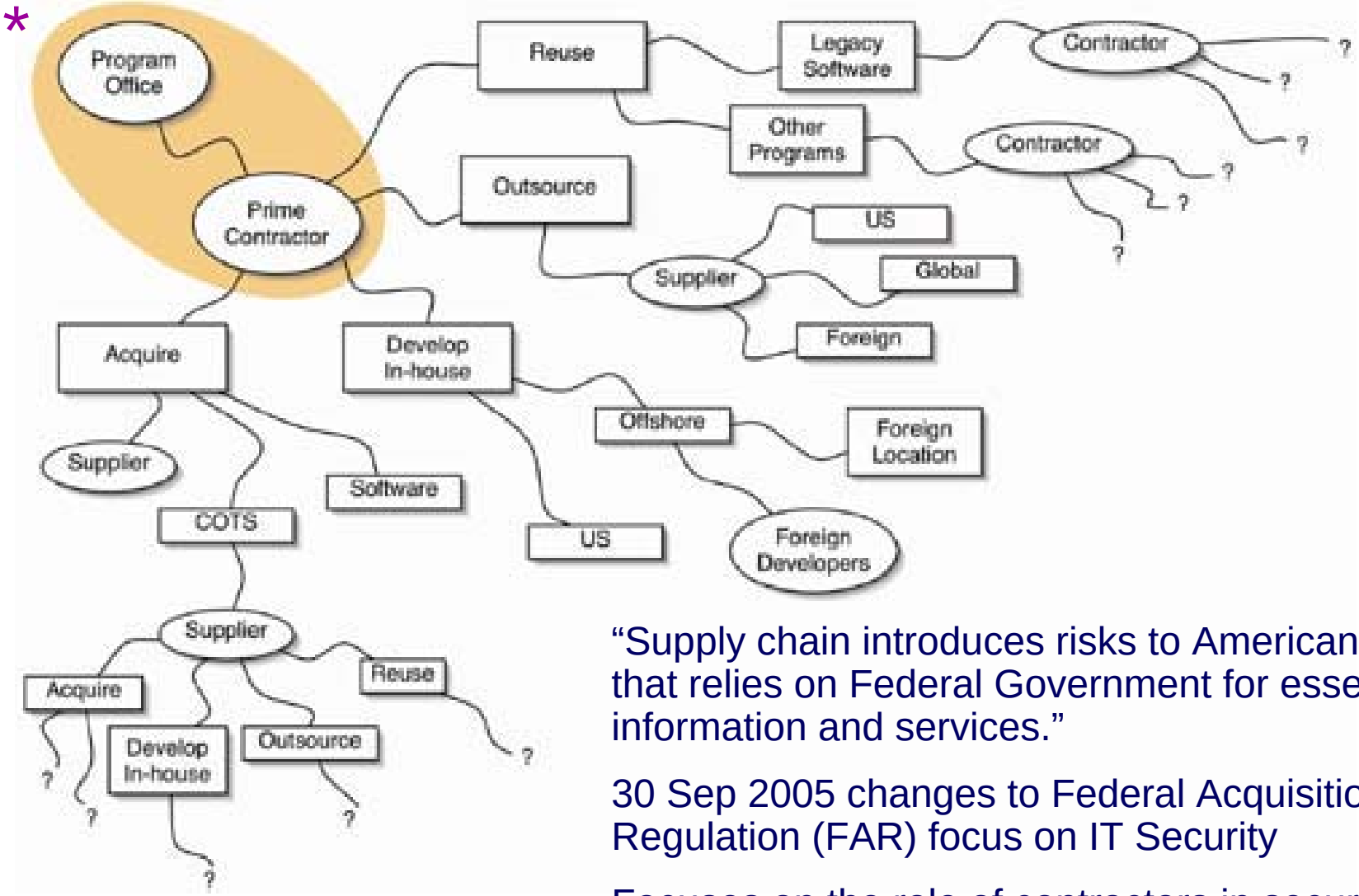
Links available via https://buildsecurityin.us-cert.gov

DHS SwA – Acquisition Focus

- Provide Software Assurance (SwA) Acquisition Guidance
  - Provided draft Acquisition Management guidance focused on enhancing supply chain management through improved risk mitigation and contracting for secure software
    - Collaborated on “due diligence” questionnaires for RFI/RFP and source selection decision making
    - Drafted templates and sample statements of work / procurement language for acquisition and evaluation based on successful models
  - Collaborated with agencies implementing changes responsive to the Federal Acquisition Regulation (FAR) IT security provisions of FISMA when buying goods and services and new core competency of “Software Acquisition Management” identified by Federal CIO Council’s IT Workforce Committee
  - Released acquisition guide, draft v1.0, “Software Assurance (SwA) in Acquisition: Mitigating Risks to the Enterprise” in March 2007 for review and comment
- Plans:
  - Co-chair IEEE CS S2ESC Working Group on updating IEEE 1062 “Software Acquisition”
  - Release acquisition guide, “Software Assurance (SwA) in Acquisition: Mitigating Risks to the Enterprise” for public review and comment in Sep 2007

Homeland Security

*



"Supply chain introduces risks to American society that relies on Federal Government for essential information and services."

30 Sep 2005 changes to Federal Acquisition Regulation (FAR) focus on IT Security

Focuses on the role of contractors in security as Federal agencies outsource various IT functions.

Homeland Security

"Scope of Supplier Expansion and Foreign Involvement" graphic in DACS www.softwaretechnews.com Secure Software Engineering, July 2005 article "Software Development Security: A Risk Management Perspective" synopsis of May 2004 GAO-04-678 report "Defense Acquisition: Knowledge of Software Suppliers Needed to Manage Risks"

Software Assurance (SwA) Acquisition Guide

"Software Assurance in Acquisition: Mitigating Risks to the Enterprise"
Draft Version 1.0 March 5, 2007

Opportunity for "Measurement in Acquisition"

Homeland Security

Software Assurance (SwA) Acquisition Guide

Appendix A— Acronyms

Appendix B— Glossary

Appendix C— An Imperative for SwA in Acquisition

Appendix D— Software Due Diligence Questionnaires (Examples)

- Table D-1. COTS Software Questionnaire
- Table D-2. Open-Source Software Questionnaire
- Table D-3. Custom Software Questionnaire
- Table D-4. GOTS Software Questionnaire
- Table D-5. Software Services

Appendix E— Other Examples of Due Diligence Questionnaires

Appendix F— Sample Language for the RFP and/or Contract

- F.1 Security Controls and Standards
- F.2 Securely Configuring Commercial Software
- F.3 Acceptance Criteria
- F.4 Certifications
- F.5 Sample Instructions to Offerors Sections
- F.6 Sample Work Statement Sections
- F.7 Open Web Application Security Project
- F.8 Certification of Originality

Appendix G— US Government Executive Branch IA Acquisition Policy & Source Code Requirements

Appendix H— References

Opportunity for “Measurement in Acquisition”

Homeland Security

DHS SwA – People Focus

- Provide Guide to Software Assurance (SwA) Common Body of Knowledge (CBK)
  - Leverage standards and “best practices” serves as a framework to guide software-related curriculum development
  - Addresses three domains: “acquisition & supply,” “development,” and “post-release assurance” (sustainment)
  - Draft v1.1 distributed on 25 Sep 2006 for review and comment; being used by early adopters in graduate level courses in secure coding/programming and NDU Information Resource Management College (IRMC) CISO Certificate Program course on SwA
  - Using common definitions from relevant standards; in collaboration with NSA/IA , updating SwA Glossary – several SwA definitions also found on-line via wikipedia.org
- Plans:
  - Next SwA CBK update with “guiding security principles” mapping to be released Sep 2007
  - Link to Common Weakness Enumeration and Common Attack Patterns - Dec 2007
  - Develop pilot training/education curriculum consistent with CBK in conjunction with early adopters for distribution by September 2008
  - Link with relevant tests, eg., SANS Secure Software Programming Assessment *
  - Provide input to IT Security Essential Body of Knowledge (EBK)

Homeland Security

Tuesday, Aug 14 in Washington DC Secure software programming tests – one on Secure Java and one on Secure C

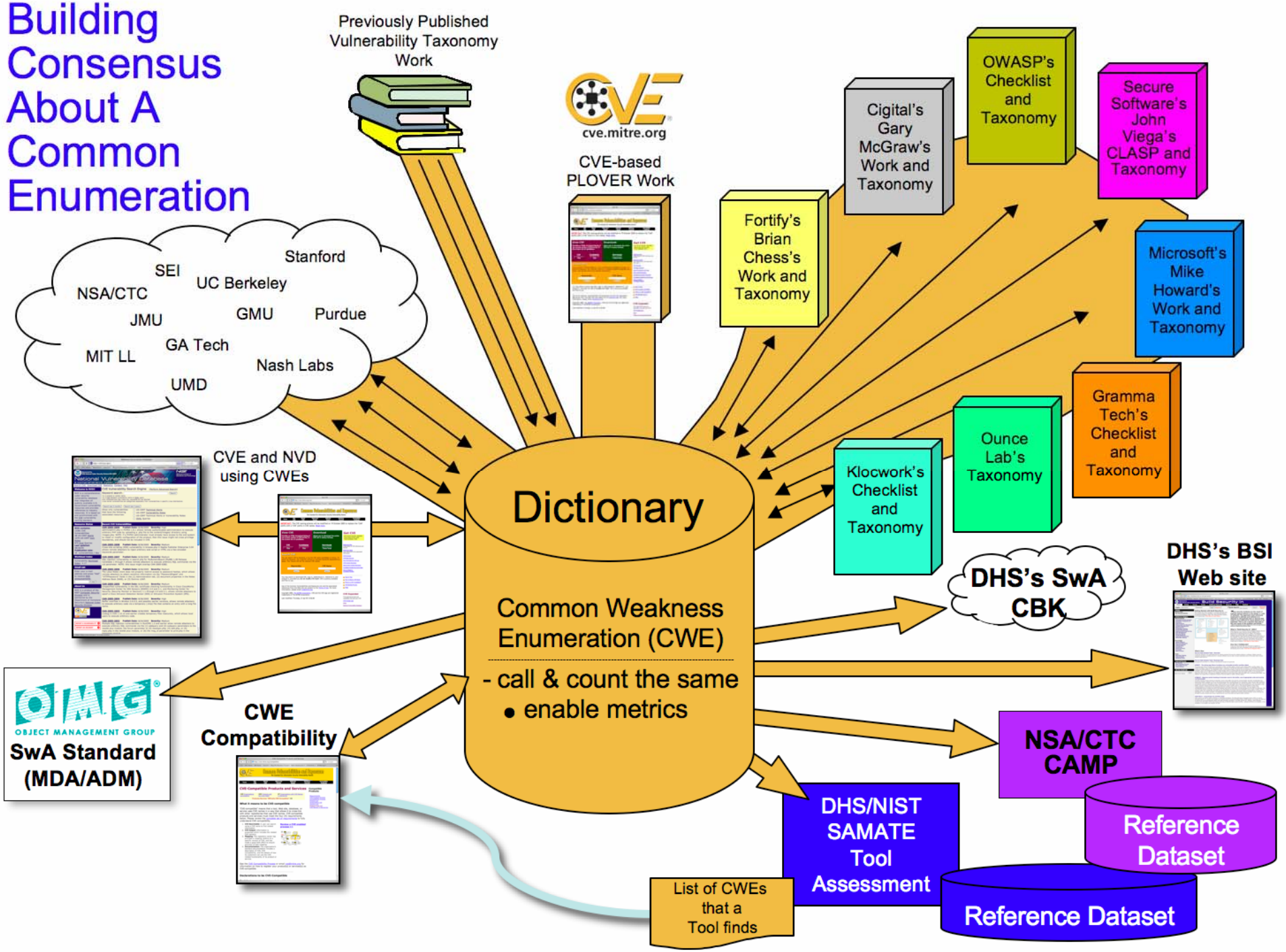
DHS SwA – Technology Focus

- Provide SwA Technology Lifecycle Support Guidance
  - Sponsor work with NIST to inventory and measure effectiveness of SwA tools
  - Sponsor public-private work to provide a common dictionary of software weaknesses (CWE) - primarily those that can be discovered by tools
  - Published common attack pattern enumeration & classification (CAPEC) with 101 attacks from which to understand resilience of software relative to abuse and misuse
  - Provide SwA Measures to support decision making throughout the software lifecycle
  - Provided draft SwA Landscape document, including organizing mechanisms for SwA ecosystem infrastructure, from which to clarify and specify interfaces and interoperability among various SwA initiatives – input to Sw Security Assurance State of the Art Report
  - NIST Special Pub 500-268, “Source Code Security Analysis Tool Functional Spec”
- Plans
  - NIST Special Pub 500-269, “SwA Tools: Web Application Scanner Functional Spec”
  - NIST Special Pub 500-270, “Source Code Security Analysis Tool Test Plan”
  - In collaboration with NIST, provide a Test Case Generator from which to evaluate SwA tool compatibility and effectiveness – demonstrated in March 2007
  - In Sep 2007 provide update draft v0.9 SwA Measurement Guide, “Practical Measurement Guidance for Software Assurance and Information Security”

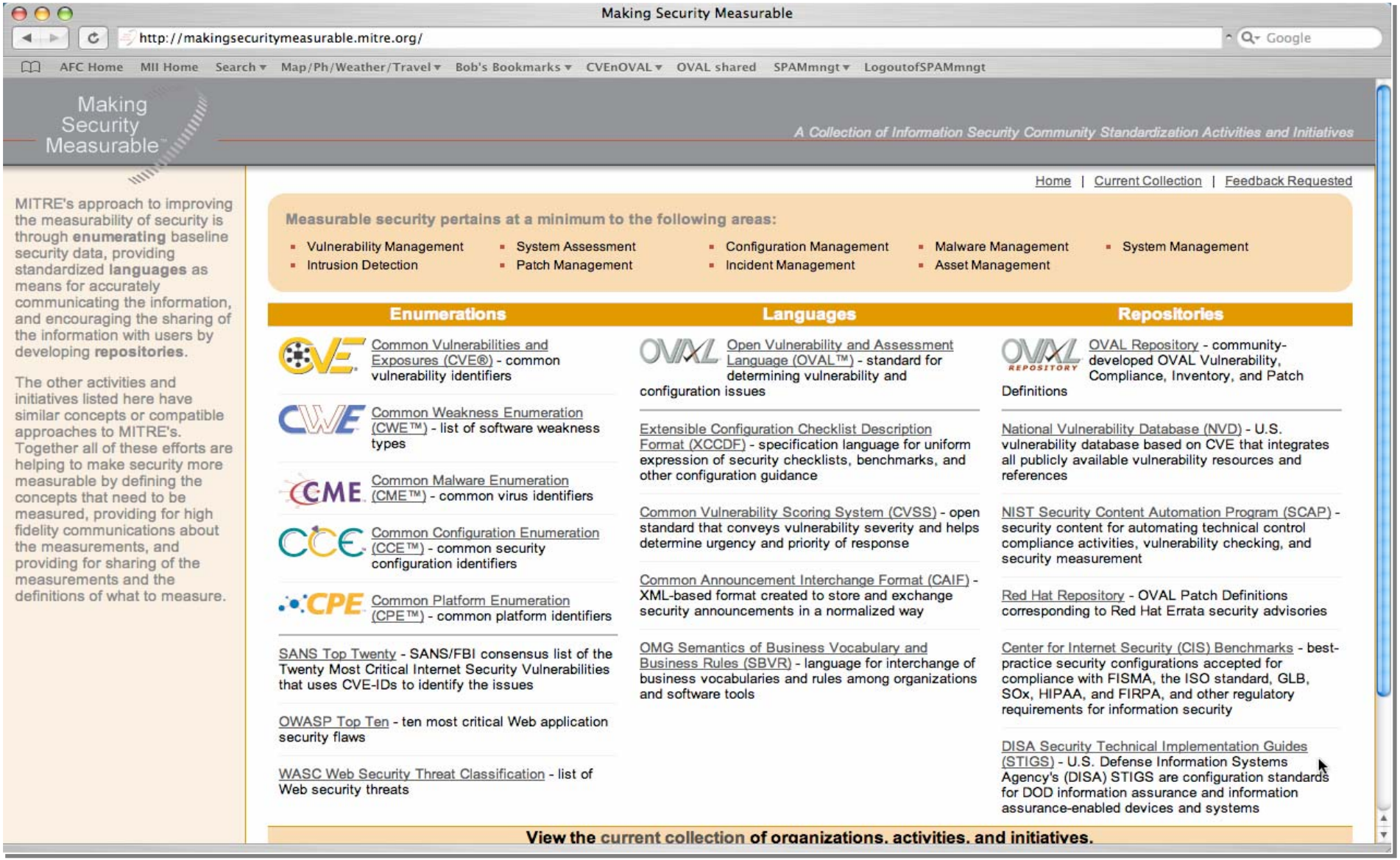
Homeland Security

A SwA Ecosystem Demonstration was held the evening of March 7, 2007 during the OMG SwA Workshop and included a demo of the Test Case Generator being co-sponsored by DHS and NIST.

Building Consensus About A Common Enumeration



For More Information [makingsecuritymeasurable.mitre.org]



DHS SwA – Process Focus

- Provide Software Assurance (SwA) Developers' Guidance
  - Provided practical guidance via "Build Security In" on US-CERT web site with regular updates based on feedback from stakeholders
  - Provided developers guide, "Securing the Software Lifecycle: Making Application Development Processes – and Software Produced by Them – More Secure" v1.2
  - Collaborate with DoD "Systems Assurance" Guidebook
  - Work with IEEE CS S2ESC, ISO/IEC JTC1 SC7/SC27/SC22, OMG, CNSS, & NIST to recommend changes to national/ international standards related to SwA
- Plans:
  - Continue to provide periodic updates to https://buildsecurityin.us-cert.gov
  - Evolve developers' guide, draft v2 in Sep 2007 reflecting new organization and references to related work
  - In collaboration with federal agencies, standards bodies, industry and academia:
    - provide draft guidance for specifying 'assurance case/arguments' from which to base claims about the safety, security and dependability of software – draft to be released September 2007 for review and comment
    - provide recommended changes to national and international standards on programming languages, software testing and software assurance
    - provide recommendations to Capability Maturity Models (CMMs) for Assurance

Homeland Security

Tues 7 Aug Workshop on Address "Assurance" with CMMI at SEI in Washington DC

Process Agnostic Lifecycle

Launched 3 Oct 2005

Architecture & Design
- Architectural risk analysis
- Threat modeling
- Principles
- Guidelines
- Historical risks
- Modeling tools
- Resources

Code
- Code analysis
- Assembly, integration & evolution
- Coding practices
- Coding rules
- Code analysis
- Resources

Test
- Security testing
- White box testing
- Attack patterns
- Historical risks
- Resources

Requirements
- Requirements engineering
- Attack patterns
- Resources

Touch Points & Artifacts

System
- Penetration testing
- Incident management
- Deployment & operations
- Black box testing
- Resources

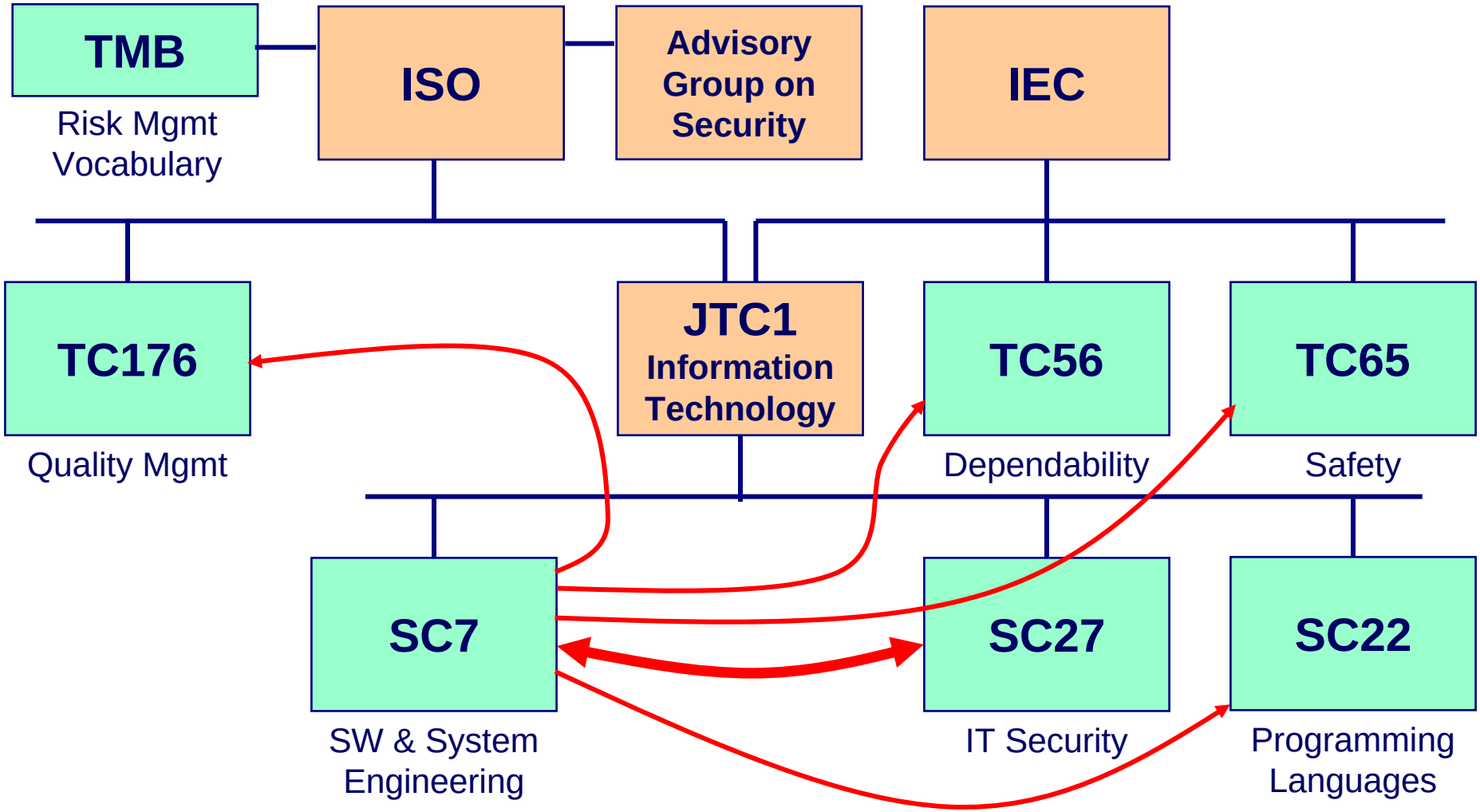
Fundamentals
- Risk management
- Project management
- Training & awareness
- Measurement
- SDLC process
- Business relevance
- Resources

Key
- Best (sound) practices
- Foundational knowledge
- Tools
- Resources

https://buildsecurityin.us-cert.gov

Homeland Security

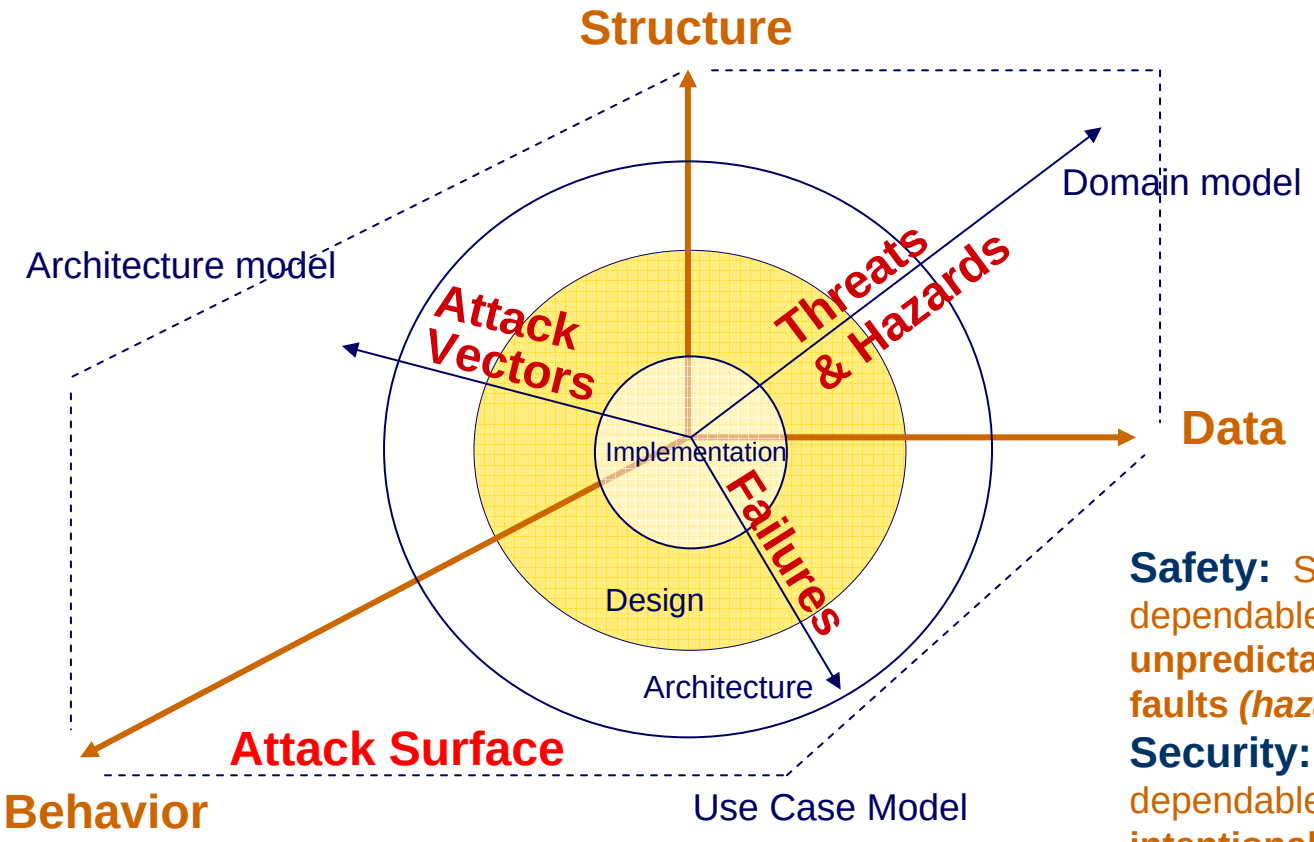
SwA Concerns of Standards Organizations



Homeland Security

* DHS NCSD has membership on SC7, SC27 & IEEE S2ESC leveraging Liaisons in place or requested with other committees

Partition of Concerns in Software-Intensive Systems



Safety: Sustaining predictable, dependable execution in the face of **unpredictable but unintentional faults *(hazards)***

Security: Sustaining predictable, dependable execution in the face of **intentional attacks *(threats)***

Considerations for Assurance Case/Arguments:

-- What can be understood and controlled (failures & attack surface/vectors)?

-- What must be articulated in terms of "assurance" claims and how might the bounds of such claims be described?

From facilitated discussions in SwA WG on Practices and Processes, Aug & Nov 2005

Scope of ISO/IEC JTC1 SC7 Software and Systems Engineering: ISO/IEC 15026 "Systems and Software Assurance"

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

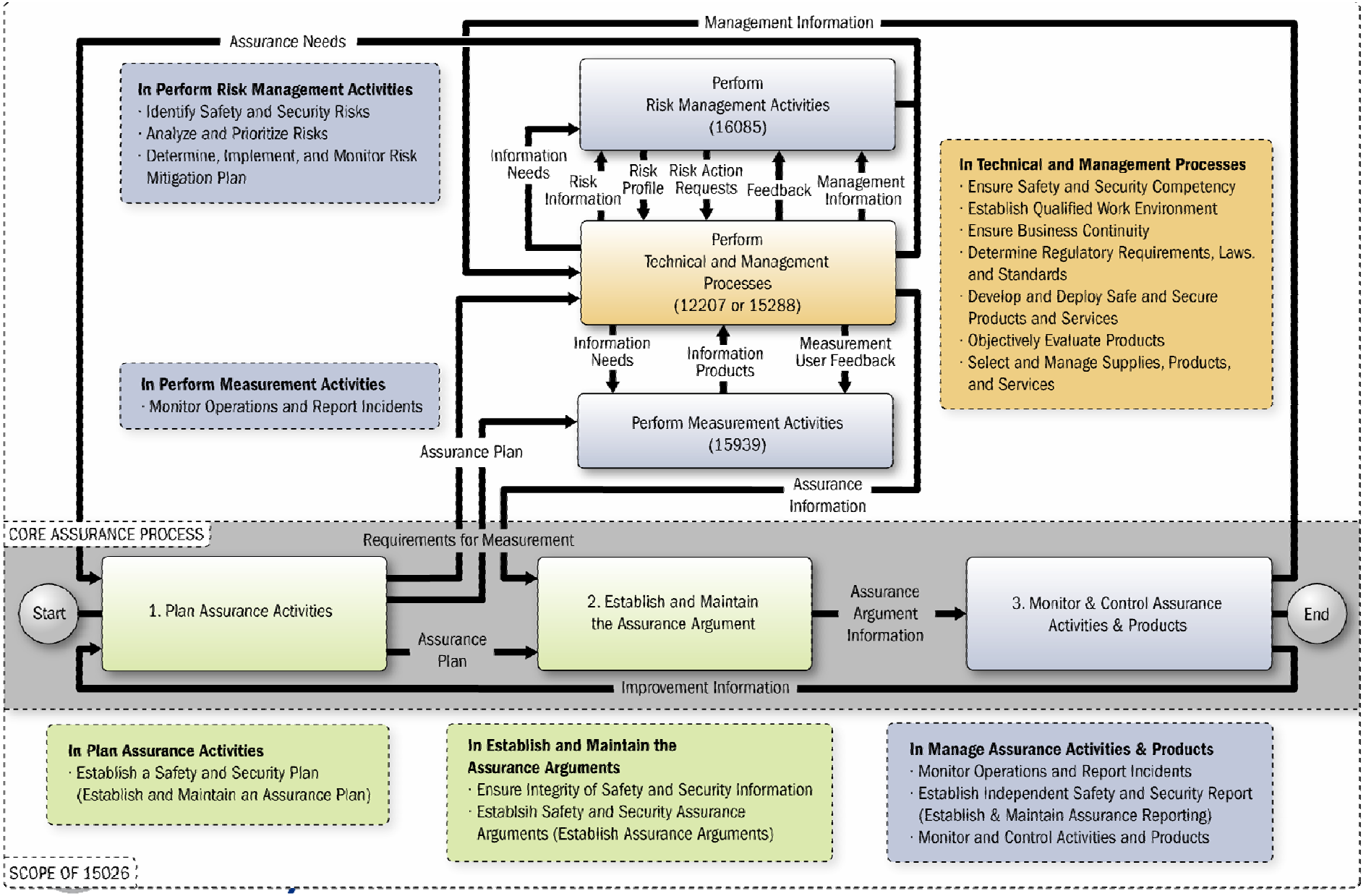
Terms of Reference changed: ISO/IEC JTC1/SC7 WG7, previously "System and Software Integrity" SC7 WG9

Status as of JTC1/SC7 Moscow Plenary 20-25 May 2007

- Appointment of IEEE CS reps as Project Editor / Co-Editor for CD ISO/IEC 15026 "Systems and Software Assurance" – out for ballot
- Liaison to JTC1/SC27/WG4 collaborative work on Application Security (N3714)

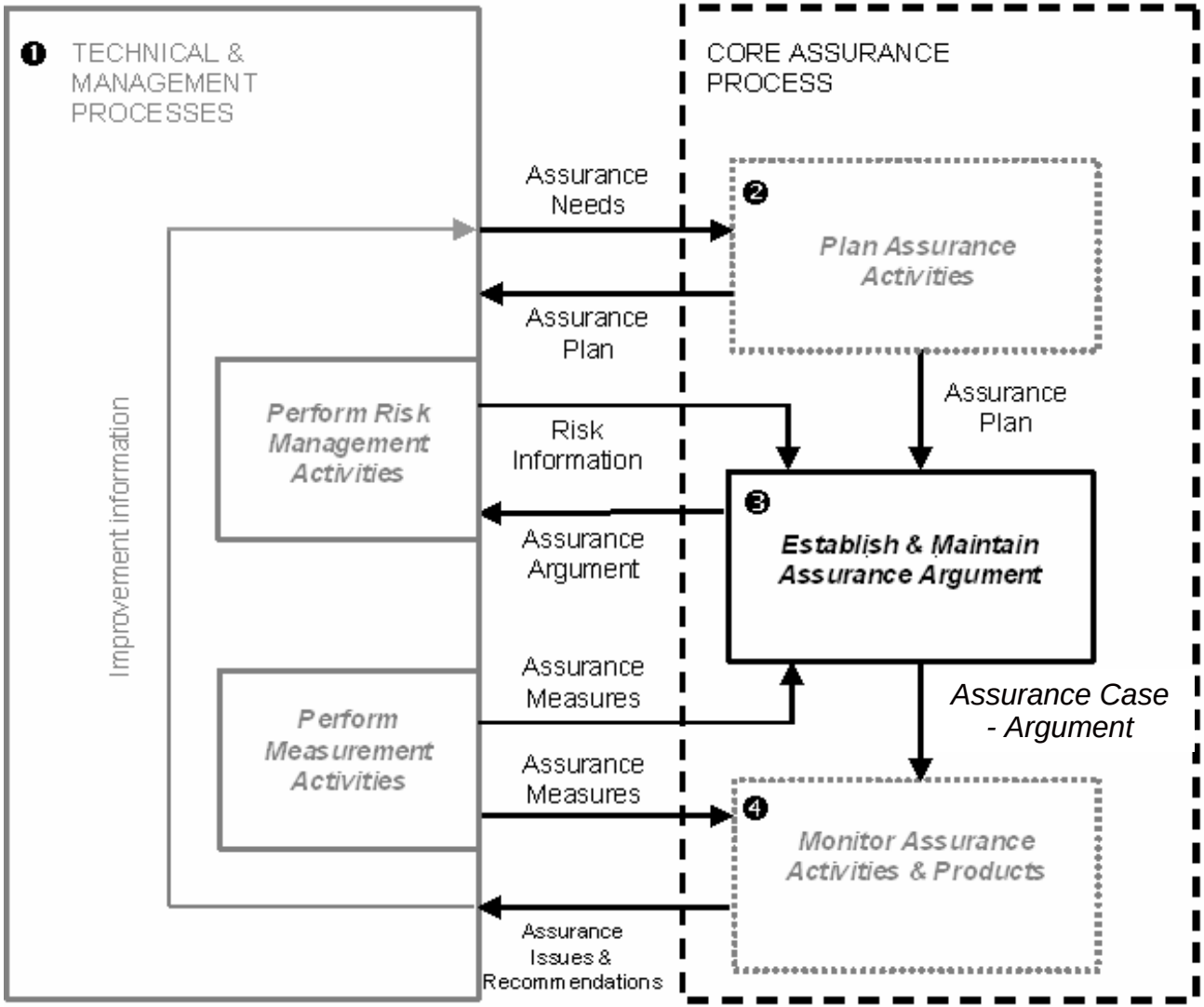
US DHS and DOD working with US suppliers to ensure consistency with related, evolving Systems and Software Assurance guidelines

ISO/IEC SC7 Framework for System & SW Assurance



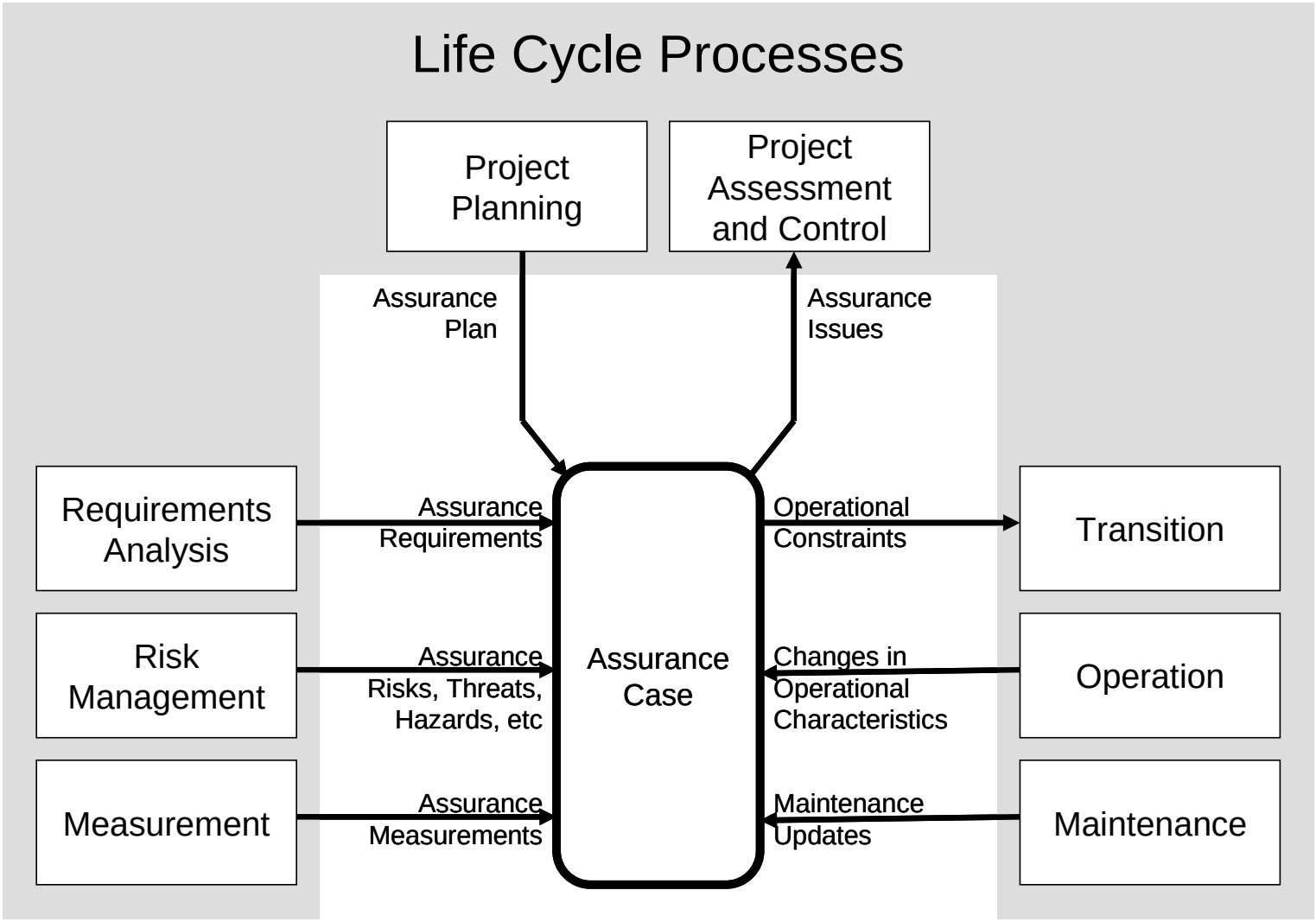
ISO/IEC JTC1 SC7 – System and Software Assurance
Interface with ISO/IEC Standards – Assurance Case/Argument

- Describes interfaces/ amplifications to the Technical & Management processes of ISO/IEC 15288 System Lifecycle & 12207 Software Lifecycle
- Describes interfaces/ amplifications to ISO/IEC 16085 Risk Management Process and 15939 Measurement Process and ISO/IEC 27004 Security Measures
- Establishes centrality of Assurance Case/Argument
- Leverages safety and IT security concepts and terminology in relevant standards



Source: ISO/IEC 15026-D4, JTC1, SC7, WG9 (currently in the process of modifying the context interrelationships)

Role of Assurance Case

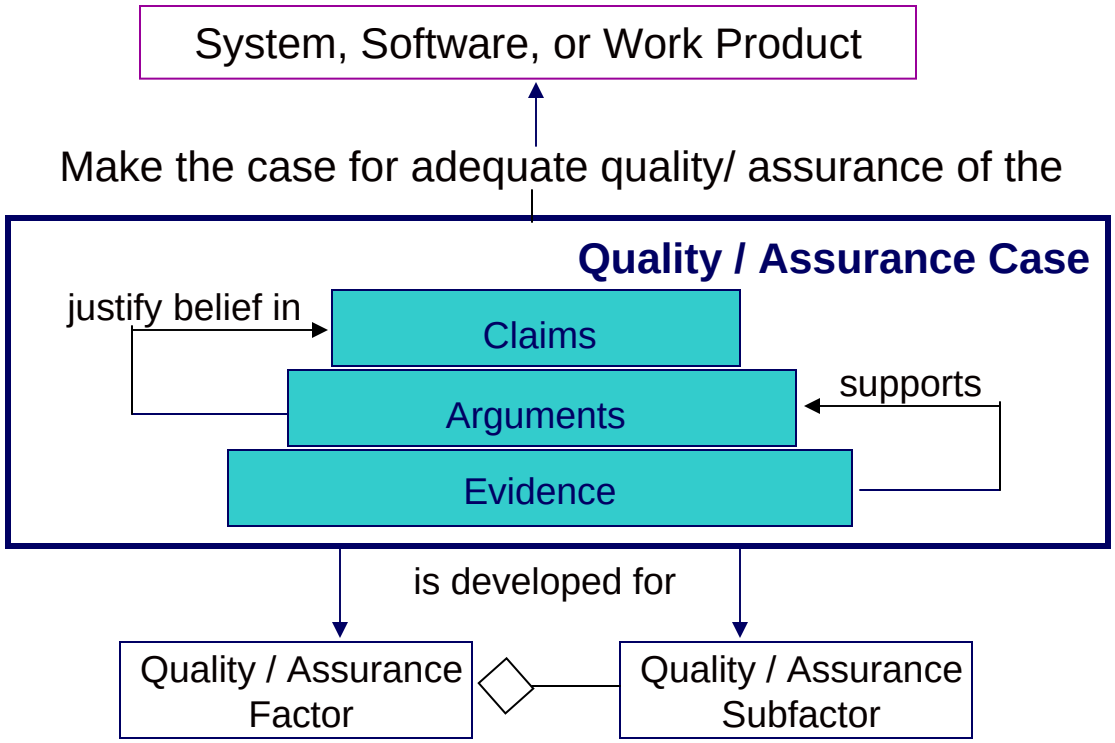


Homeland Security

Making an ISO/IEC 15026 "Conformant" Assurance Case/Claim --

What constitutes sufficient Evidence to support Arguments that justify Claims?

How might "scaling" be structured to enable and encourage more suppliers and acquirers to make use of assurance cases?



Homeland Security

Adopted from US TAG ISO/IEC 15026 proposal May 2007 and CMU SEI QUASAR tutorial by Donald Firesmith, March 2007

What if…

- An overarching scheme for evaluating suppliers and products leveraged standards and CMMs to understand and mitigate risk exposures
  - Assurance Cases enabled “scaling”:
    - Formal methods
    - Internationally recognized product evaluation schemes, eg. Common Criteria
    - Qualified tool-based evaluations (with test results independently verified)
  - Harmonized use of standards and CMMs enabled suppliers and acquirers to better leverage investments in process improvement to support needs for “assurance” in products and systems
  - Measurement adequately supported information needs to facilitate the use of assurance cases

Homeland Security

General Requirements on Assurance Cases

- The project shall establish and maintain an assurance case.
- The project shall ensure that:
  - Goals and objectives for safety, security, dependability and any other designated critical properties are formulated.
  - Product assurance-related objectives, properties, or characteristics are explicitly selected for special attention and application of this standard to address the goals and objectives.
  - Requirements for the achievement of these objectives, properties, or characteristics are defined.
  - **Measures for the requirements are selected and related to the desired characteristics.**
  - Criteria for the achievement or degree or achievement of these objectives, properties, or characteristics are selected and traced to requirements.
  - Approaches for achieving the objectives, properties, or characteristics are planned, designed, and implemented, as well as demonstrating and documenting that achievement.
  - The extent of achievement is continuously monitored, documented, and communicated to stakeholders and managers.
  - An assurance case documenting and communicating the extent of achievement is specified, developed, and maintained as an element of the system.
  - The artifacts for documenting, analyzing, and communicating the required or claimed properties and characteristics and the extent of achievement are specified, developed, and maintained.
  - Requirements of the approval authority are satisfied and necessary licenses or certifications are received.

Homeland Security

Measurement in ISO/IEC 15026

- Assurance claim must use measures and be measurable
- Assurance claims must be characterized in terms of critical performance parameters
  - Ability to compromise the system
  - Management of tolerance thresholds
  - Characterize appropriate balance between assurance and functionality – it's a trade off
- Two types of measures are required
  - Reflecting the achievement of assurance objectives
    - Binary (y/n)
    - Extent of achievement
    - Completeness of processes
  - Reflecting the effectiveness of assurance processes and procedures
    - Degree of residual risk (probability)
    - Efficiency and effectiveness of processes
    - Link to higher levels of CMMI (Level 4/5) and predicative models

Homeland Security

ISO/IEC SC27 ISMS Family of Standards

- A management system for information security, similar to ISO 9000 for quality management and ISO 14000 for environmental quality management
- First introduced by the British Standards Institute (BSI) as a part of BS-7799 multipart standard
- Evolved into two ISO/IEC standards –
  - ISO/IEC 27001, *Information Security Management System – Requirements*, that provides a process for planning, implementing, monitoring, and improving an ISMS and a minimum set of security controls
  - ISO/IEC 27002, *Code of Practice for Information Security*, that provides guidance on security controls provided in ISO/IEC 27001

Homeland Security

ISO/IEC 27004 – one of the ISMS standards under development

ISO/IEC 27000 - *ISMS Overview and Vocabulary*	Foundational standard in the 27000 series. Progressing through technical level voting. Expected publication is in 2008.
ISO/IEC 27003 – *Information Security Management System Implementation Guidance*	Provides further guidance on implementing 27001. Under development. Expected publication in 2008.
ISO/IEC 27004 – *Information Security Management Measurement*	Provides guidance on measuring effectiveness of security program implementation, as required by 27001 and 27002. Expected publication is in 2008.
ISO/IEC 27005 – *Information Security Risk Management*	Provides guidance on conducting risk assessment and managing risk, as required by 27001 and 27002. Progressing through committee voting. Expected publication is in 2008.
ISO/IEC 27007 – *ISMS Auditing Guidelines*	Study Period on the subject was closed with a recommendation to develop New Proposal. China and Sweden submitted contributions and presented at the meeting. New Proposal will be coming out in the next 2 months with an outline for the new standard. Work is expected to commence after October meeting.
ISO/IEC 27011 (ITU-T X.1051) – *Information Security Management Guidelines for Telecommunications*	Joint publication with ITU-T to update current telecommunications industry standard (ITU-T X.1051) to be consistent with ISO/IEC 27001. Several member bodies objected under grounds that multiple ISMS requirements standards complicate compliance. Compromise was worked out, development is progressing.
ISMS Technical Audit Study Period	Study period was initiated to explore the subject with a potential outcome of developing a standard. The subject matter seems to be closely related to security assessments and NIST SP 800-53A.
Sector-Specific ISMS Standards	World Lottery Association (WLA) and Automotive Industry Study Periods were extended. Other industries have begun creating their own variants of the standards. WG1 is in the process of putting together a strategy to mange proliferation of Sector-Specific ISMSs.

ISO/IEC 27004 is Aligned with PSM

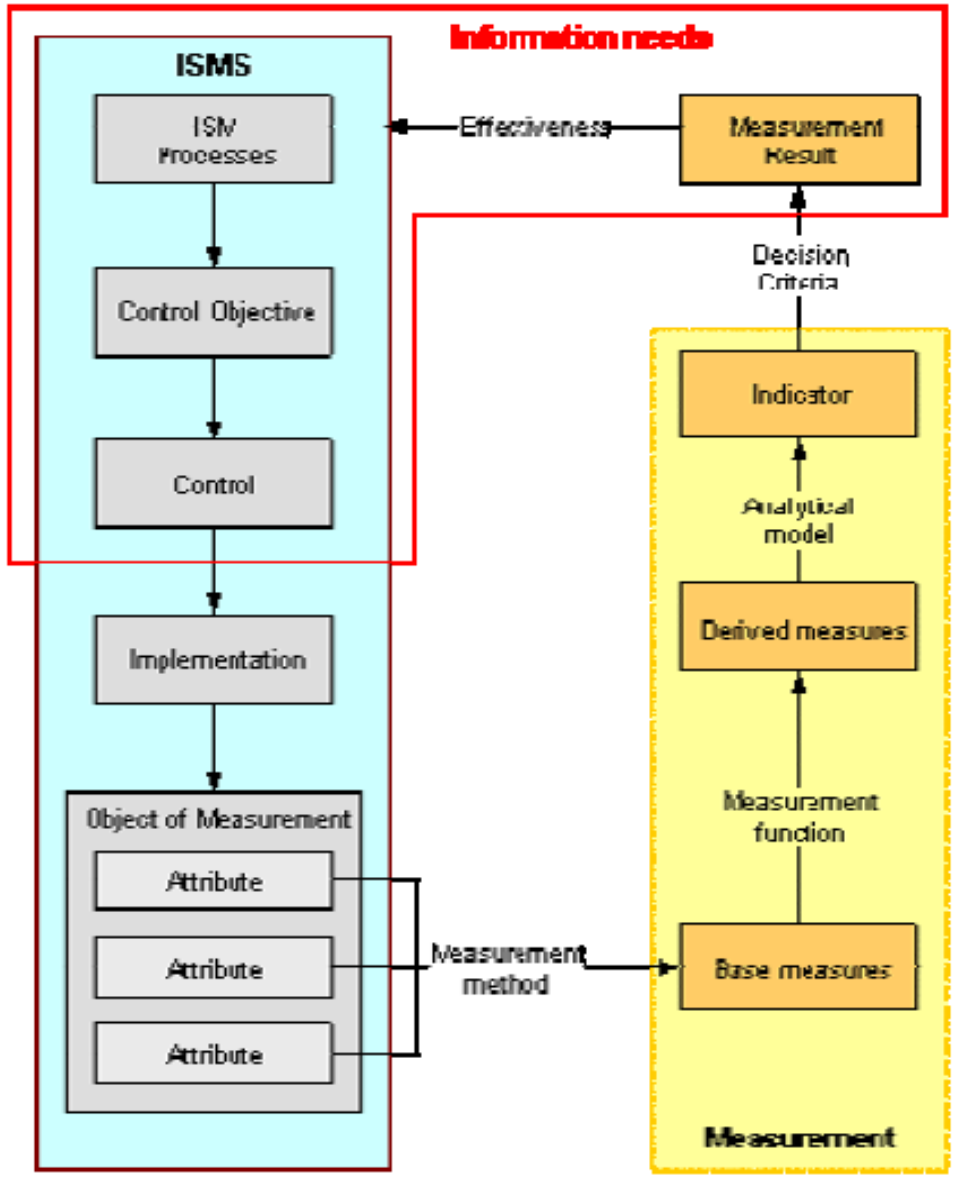


Figure — 2 Information Security Measurement Model

Homeland Security

SwA Measurement Working Group Status

- Measurement Guidance is under revision to be released for review (draft by Sep 2007)
  - Common measurement framework
  - High level measurement process
  - Key measures examples
- A set of resources will be published on the SwA web site in July-September 2007
  - Targeting primary stakeholder groups: Executive, Developer/Vendor/Supplier, Buyer/Acquirer
  - Goals and questions lists
  - Sources of measurable requirements
  - Links to likeminded efforts (PSM, CMMI, etc.)
  - Articles on SwA measurement, security measurement, and software security measurement
  - Measurement methodologies
  - Measures lists
  - Measures examples with filled out specs/templates and crosswalks of multiple methodologies
  - Automated tools listings

Opportunity for PSM involvement and web site linkage

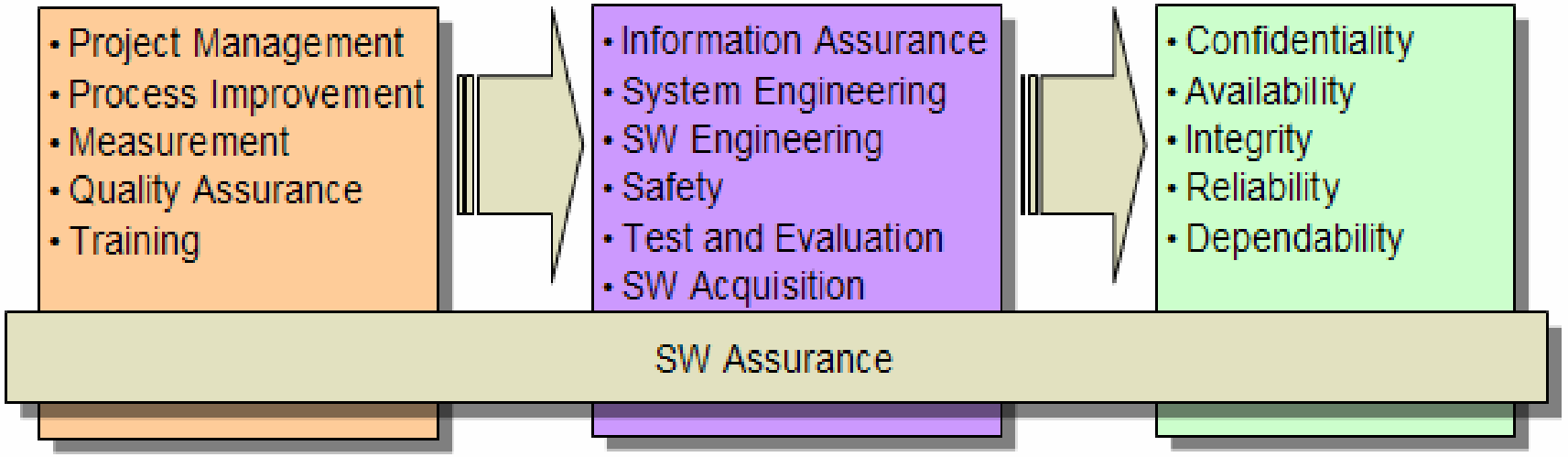
Homeland Security

SwA Measurement Guidance: Purpose

- To provide a practical framework for measuring software assurance achievement of SwA goals and objectives within the context of individual projects, programs, or enterprises.
  - Making informed decisions in the software development lifecycle related to information security compliance, performance, and functional requirements/controls
  - Facilitate adoption of secure software design practices
  - Respond to identified threats throughout the System Development Lifecycle (SDLC) and ultimately reduce the numbers of vulnerabilities introduced into software code during development
  - Determining if security/performance/trade-offs have been defined and accepted
  - Assessing the trustworthiness of a system.
- Can be applied beyond SwA to a variety of security-related measurement efforts to help facilitate risk-based decision making through providing quantitative information on a variety of aspects of organization's security related performance.

SwA Measurement Guidance: Scope

- Covers the most under-developed aspects of SwA measurement, which pertain to measuring the trustworthiness of the developed code.
- Leverages existing methodologies, used in the software development and system integration fields, as well as existing and evolving methodologies used in the information security field.



Homeland Security

SwA Measurement Guidance: Key Definitions

- Software Assurance: The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and the software functions in the intended manner. [CNSS Instruction No. 4009]
- Measure: Variable to which a value is assigned as the result of measurement [ISO/IEC 15939]
- Measurement: Set of operations having the object of determining a value of a measure [ISO/IEC 15939]

SwA Measurement Guidance: Key Principles

- SwA measurement must satisfy information needs of a variety of stakeholders/audiences, including executive decision makers, vendors/developers/suppliers, and acquisition professionals.
- Each stakeholder group will require tailoring of specific measures based on each group's information needs.
- Different measures targeting different stakeholders may use the same information originating from the same data sources this facilitating single data entry and multiple reuses.
- Each phase of the SDLC, acquisition life cycle, or any other life cycle introduces an opportunity to measure SwA and improve its results.
- For the purposes of this document, the term "measurement" applies to both quantitative and qualitative measurement methodologies.

Homeland Security

SwA Guidance: Stakeholders

- Acquisition professionals
- Vendors/developers/suppliers
- Executive decision makers

SwA Measurement tools and resources are tailored to these stakeholders' perspectives

Homeland Security

	Software & Systems			Information Security	
	PSM ISO/IEC 15939	CMMI (Measurement and Analysis Process Area)	CMMI GQ(I)M	ISO/IEC 27004	NIST SP 800-55
Approach	**Methodology:** Information Need driven. **Purpose:** To align Information Needs with Indicators and Measures.	**Purpose:** To develop and sustain a measurement capability that is used to support management information needs.	**Methodology:** Goal driven. **Purpose:** To align Goals with Indicators and Measures.	**Purpose:** To guide an organization through the use of information security measurements, identifies the adequacy of an existing ISMS, including policy, risk management, control objectives, controls, processes and procedures.	**Purpose:** To guide the specific development, selection, and implementation of information system-level and program-level measures to be used to indicate the effectiveness of security controls applied to information systems and supporting information security programs.
Goal/Objective/Information Need Description	**Information Need:** What the measurement user (e.g., manager or project team member) needs to know in order to make informed decisions.	**SG 1: SP 1.1** Establish measurement objectives.	**Objective:** Describe the objective or purpose of the indicator.	**Purpose of measure:** Defines the goal of collecting and reporting the measure	**Goal and Objective:** Statement of information security goal and objective. For system-level security control measures, the goal would guide security control implementation for that information system. For programmatic measures, both strategic goals and information security goals can be included. For example, information security goals can be derived from enterprise-level goals in support of the organizations mission. These goals are usually articulate in strategic and performance plans. When possible, include both the enterprise-level goal and the specific information security goal extracted from agency documentation, or identify an information security program goal that would contribute to the accomplishment of the selected strategic goal or objective.
	Information Category: A logical grouping of information needs that are defined in the PSM to provide structure for the Information Model. PSM categories include schedule and progress, resources and cost, product size and stability, product quality, process performance, technology effectiveness, and customer satisfaction. Categories are defined in Chapter 2 of the PSM book.			**Control or Control Objective:** Control or control objective under measurement.	
Measurable Concept/Question	**Measurable Concept:** An abstract relationship between attributes of entities and information needs.		**Question: List the question(s) the indicator user is trying to answer. Probing Questions: List questions that delve into the possible reasons for the value of an indicator, whether performance is meeting expectations or whether appropriate action is being taken.**		
Entities/Attributes	**Relevant Entities:** The object that is to be measured. Entities include process or product elements of a project such as project tasks, plans/estimates, resources, and deliverables.		**Inputs - Data Elements:** List all data elements in the production of the indicator. **Inputs - Definition:** Precisely define the data element used or point to where the definition can be found.	**Object of Measurement:** The object that is to be measured. Objects may include processes, systems, or system components.	
	Attributes: The property or characteristic of any entity that is quantified to obtain a base measure.		**Inputs - Data Elements:** List all data elements in the production of the indicator.	**Attributes:** property or characteristic of an object of measurement that can be distinguished quantitatively or qualitatively by human or automated means	

Base Measure Specification	**Base Measure:** A base measure is a measure of a single attribute defined by a specified measurement method (e.g., planned number of lines of code, cumulative cost to date). As data is collected, a value is assigned to a base measure.		**Inputs - Data Elements:** List all data elements in the production of the indicator.	**Base Measure:** A base measure is a measure of a single attribute defined by a specified measurement method (e.g., number of trained personnel, number of sites, cumulative cost to date). As data is collected, a value is assigned to a base measure.
				Numerical identifier: Unique organization-specific numerical identifier
				Measure Name: Measure Name
	Measurement Method: The logical sequence of operations that define the counting rule to calculate each base measure.		**Data Collection - How:** Describe how the data will be collected.	**Measurement Method:** The logical sequence of operations that define the counting rule to calculate each base measure.
	Type of Method: The type of method used to quantify an attribute, either (1) subjective, involving human judgment, or (2) objective, using only established rules to determine numerical values.	**SG 1: SP 1.2** Specify Measures.	**Data Collection - How:** Describe how the data will be collected.	
	Scale: The ordered set of values or categories that are used in the base measure.	**SG 1: SP 1.2** Specify Measures.	**Inputs - Definition:** Precisely define the data element used or point to where the definition can be found.	**Scale:** The ordered set of values or categories that are used in the base measure.
	Type of Scale: The type of relationship between values on the scale, either: - Nominal: the measurement values are categorical, as in defects by their type. - Ordinal: the measurement values are rankings, as in assignment of defects to a severity level. - Interval: the measurement values have equal increments for equal quantities of the attribute, such as an additional cyclomatic complexity value for each additional logic path in the software unit. - Ratio: the measurement values have equal increments, beginning at zero, for equal quantities of the attribute, such as size measurement in terms of LOC.	**SG 1: SP 1.2** Specify Measures.	**Inputs - Definition:** Precisely define the data element used or point to where the definition can be found.	**Scale:** The ordered set of values or categories that are used in the base measure.
	Unit of Measurement: The standardized quantitative amount that will be counted to derive the value of the base measure, such as an hour or a line of code.	**SG 1: SP 1.2** Specify Measures.	**Inputs - Definition:** Precisely define the data element used or point to where the definition can be found.	
Derived Measure Specification	**Derived Measure:** A measure that is derived as a function of two or more base measures.	**SG 1: SP 1.2** Specify Measures. **SG 2: SP 2.1** Collect Measurement Data.	**Inputs - Data Elements:** List all data elements in the production of the indicator.	**Derived Measure:** A measure that is derived as a function of two or more base measures.
	Measurement Function: The formula that is used to calculate the derived measure.	**SG 1: SP 1.2** Specify Measures.	**Algorithm:** Specify the algorithm or formula required to combine data elements to create input values for the indicator. It should also include	**Measurement Function:** The formula that is used to calculate the derived measure.

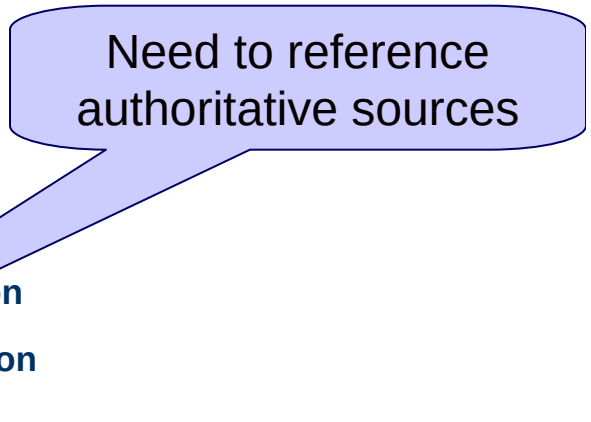
Indicator Specification	**Indicator Description and Sample:** A display of one or more measures (base and derived) to support the user in deriving information for analysis and decision making. An indicator is often displayed as a graph or a chart. Include a sketch of the indicator.	**SG 1: SP 1.2** Specify Measures. **SG 2: SP 2.2** Analyze Measurement Data.	**Indicator:** An indicator is defined as a measure or a combination of measures that provides insight into a process, a project, or a product. An indicator is usually a graph or table that you define for the organization's needs. **Visual Display:** Provide a graphical view of the indicator.	**Indicator Description and Sample:** A display of one or more measures (base and derived) to support the user in deriving information for analysis and decision making. An indicator is often displayed as a graph or a chart. Include a sketch of the indicator.
	Analysis Model: A process that applies decision criteria to define the behavior responses to the quantitative results of the indicator.	**SG 1: SP 1.2** Specify Measures. **SG 2: SP 2.2** Analyze Measurement Data.	**Analysis:** Specify what type of analysis can be done with the information.	**Analysis Model:** A process that applies decision criteria to define the behavior responses to the quantitative results of the indicator.
	Decision Criteria: A defined set of actions that will be taken in response to achieved quantitative values of the model.	**SG 1: SP 1.4** Specify Analysis Procedures. **SG 1: SP 1.4** Specify Analysis Procedures.		**Decision Criteria:** A defined set of actions that will be taken in response to achieved quantitative values of the model.
	Indicator Interpretation: A description of how the sample indicator (see sample figure in indicator description) was interpreted.	**SG 2: SP 2.2** Analyze Measurement Data. **SG 2: SP 2.4** Communicate Results	**Interpretation:** Describe what different values of the indicator mean. Make it clear how the indicator answers the "Questions" section above. Provide any important cautions about how the data could be misinterpreted and measures to take to avoid misinterpretation.	**Indicator Interpretation:** A description of how the sample indicator (see sample figure in indicator description) was interpreted. **Effects/Impact:** Definition of the effects and impact derived as a consequence of the results obtained by the measure **Causes of deviation:** Definition of possible causes that may originate deviations in the results obtained **Positive values:** It is specified whether increasing values indicate positive values (good result) or whether decreasing values are to be taken to indicate positive values **Reporting formats:** Reporting format should be identified and documented. Describes the observations that the organization or owner of the information may want on record. Reporting formats will visually depict the measures and provide a verbal explanation of the indicators.

Example Measure 1

- Information Category: System Development
- Measurable Concept: Design
- **Measure: # of entry points for a module (should be as low as possible)**
- **Measure: # exit points for a module (should be 1)**
- Information Need/Goal: Understand the level of exposure from back doors
- Question: Have we reduced exposure from back doors to minimal level?
- Additional information: Low number of entry points reduces opportunities for back doors

Homeland Security

Example Measure 2



- Information Category: System Development
- Measurable Concept: Development
- **Measure: # of discovered defects that may effect predictable execution**
- **Measure: # places user input is requested and extent of input validation**
- **Measure: # of times high risk commands are used**
- **Measure: # of flaws per area of the code in which they were found**
- Information Need/Goal: Minimize development and maintenance rework costs caused by security-related flaws and reduce chances of intentional system misuse
- Question: Have security flaws been addressed prior to testing and deployment?

Example Measure 3

- Information Category: System Development
- Measurable Concept: Requirements Management
- **Measure:** *Seeking a good measure. Requirements traceability is a decent proxy but does not help ensure that security was integrated from day one.*
- Information Need/Goal: Have appropriate security requirements been integrated into the system?
- Question: Have appropriate functional and non-functional security requirements have been identified and documented?

Homeland Security

Example Measure 4

- Information Category: System Development
- Measurable Concept: Testing
- **Measure: % of modules that contain defects that may effect predictable execution of total modules**
- **Measure: % of failed security controls of total required**
- Information Need/Goal: Gain insights into risk of the system being exploited when operational
- Question: Does the system contain software defects that may be exploited in the future?

Homeland Security

Security in the Software Life Cycle:
Informed development and supply chain management

- Enhance existing processes, methods and technologies to help specify, design, implement, configure, evaluate, & sustain software that is able to:
  - Resist or withstand many anticipated attacks.
  - Recover rapidly and mitigate damage from attacks.
- Keys to secure software:
  - A security-enhanced software development life cycle process -- includes practices and technologies that help developers root out and remove exploitable defects (e.g., weaknesses and vulnerabilities) and increase the likelihood that such defects will not be introduced in the first place.
  - A security-enhanced acquisition / out-sourcing life cycle process -- includes practices that address risks associated with the software supply chain (including due-diligence practices that assist in mitigating risk exposures posed by software and suppliers)

Functional Correctness must be exhibited even when software is subjected to hostile conditions; therefore, claims about system reliability, integrity and safety must include provisions for built-in security of enabling software

What if…

- **Government, in collaboration with industry / academia, raised expectations for product assurance with requisite levels of integrity and security:**
  - Helped advance more comprehensive software assurance diagnostic capabilities to mitigate risks stemming from exploitable vulnerabilities and weaknesses;
  - Promoted use of methodologies and tools that enabled security to be part of normal business.
- **Acquisition managers & users factored risks posed by the supply chain as part of the trade-space in risk mitigation efforts:**
  - Information on suppliers' process capabilities (business practices) would be used to determine security risks posed by the suppliers' products and services to the acquisition project and to the operations enabled by the software.
  - Information about evaluated products would be available, along with responsive provisions for discovering exploitable vulnerabilities, and products would be securely configured in use.
- **Suppliers delivered quality products with requisite integrity and made assurance claims about the IT/software safety, security and dependability:**
  - Relevant standards would be used from which to base business practices & make claims;
  - Qualified tools used in software lifecycle enabled developers/testers to mitigate security risks;
  - Standards and qualified tools would be used to certify software by independent third parties;
  - IT/software workforce had requisite knowledge/skills for developing secure, quality products.

Homeland Security

… this requires Measurement

Software Assurance

Information clearinghouse for topics related to Software Assurance

Sponsored by DHS National Cyber Security Division

- Home
- People
- Process
- Technology
- Acquisition
- Working Groups
- RSS feeds
- Overview
- Join a Working Group

Launch http://us-cert.gov/SwA for Software Assurance Community of Practice (Summer 07)

Build Security In

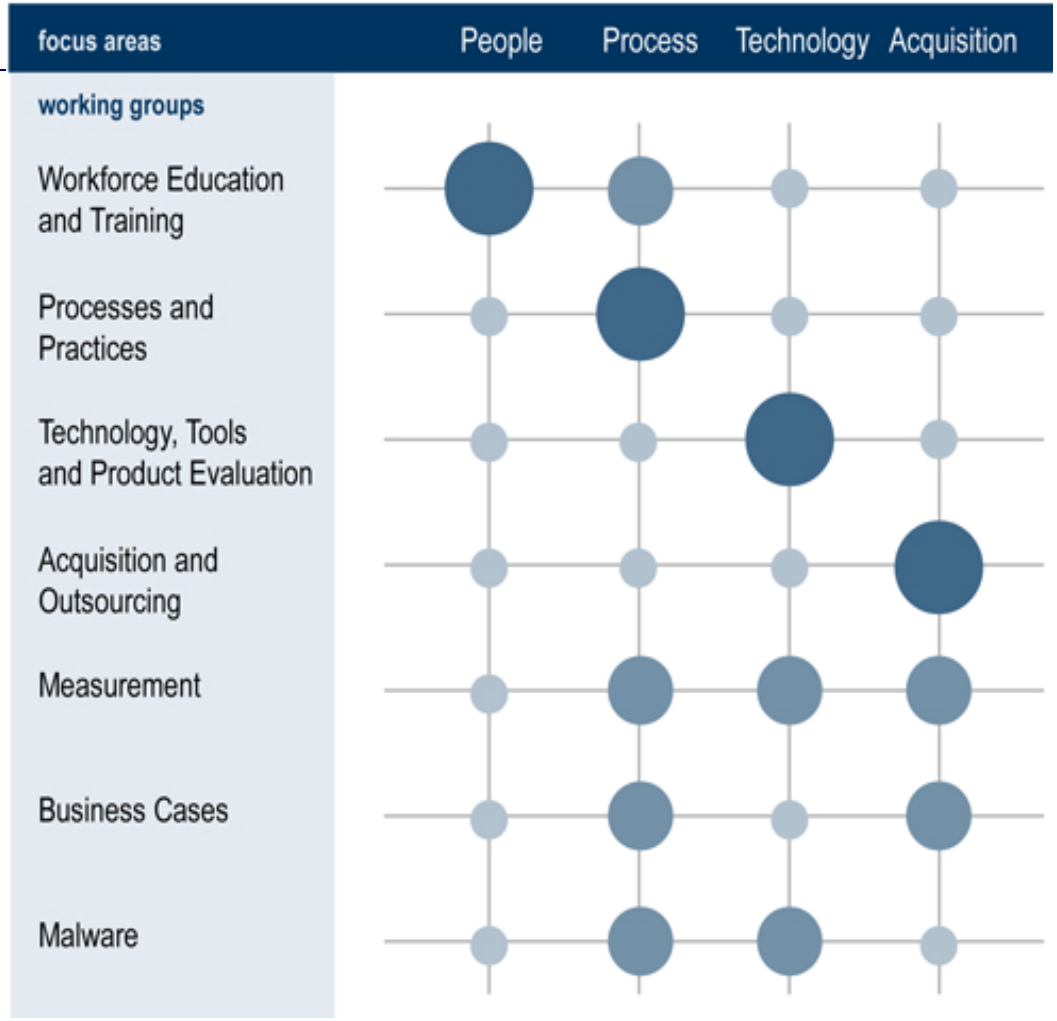
Find the information you need to navigate the security landscape.
Get started now!

WORKING GROUPS

SwA Working Groups are created to give focus to specific areas within the effort. More description would live here in this paragraph. A comprehensive description would provide information to the user to determine what is the purpose of working groups and what they are like. It might also reference results of the working group activity here in this area as an example.

And perhaps briefly outline the different levels of participation: active and observer.

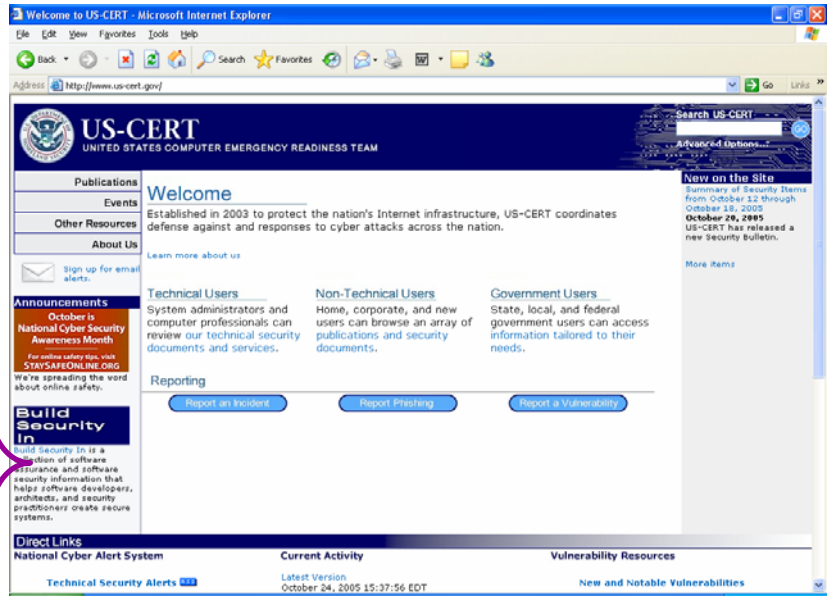
Software Assurance Focus and Working Group Matrix



SwA Working Group Sessions every two months – Next 4-6 Dec 2007

Next SwA Forum 2-3 Oct 2007 at Hilton, McLean, VA

www.us-cert.gov →



See http://us-cert.gov/SwA for SwA Community of Practice

http://buildsecurityin.us-cert.gov

Joe Jarzombek, PMP
Director for Software Assurance
National Cyber Security Division
Department of Homeland Security
Joe.Jarzombek@dhs.gov
(703) 235-5126

Homeland Security

Homeland Security

Questions?