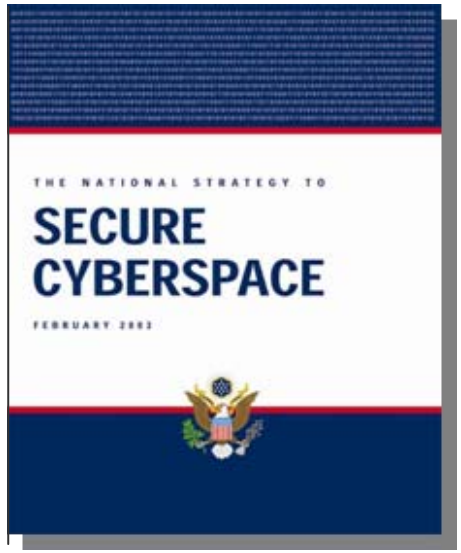
Software Assurance:

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



Considerations in Advancing the National Strategy to Secure Cyberspace

June 26, 2006

Homeland Security

Joe Jarzombek, PMP
Director for Software Assurance
National Cyber Security Division
US Department of Homeland Security

What if…

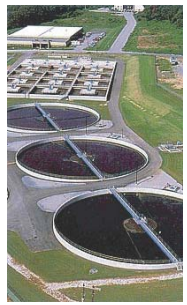
- **Government, in collaboration with industry / academia, raised expectations for product assurance with requisite levels of integrity and security:**
  - Structured and funded to advance more comprehensive software assurance diagnostic capabilities to mitigate risks stemming from exploitable vulnerabilities;
  - 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 throughout the lifecycle.
- **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;
  - IT/software workforce had requisite knowledge/skills for developing secure, quality products;
  - Sales increased in the public and private sectors that demanded high assurance products.

Homeland Security

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

- Chemical Industry
  - 66,000 chemical plants

- Banking and Finance
  - 26,600 FDIC institutions
- Agriculture and Food
  - 1.9M farms
  - 87,000 food processing plants



- Water
  - 1,800 federal reservoirs
  - 1,600 treatment plants

- Public Health
  - 5,800 registered hospitals
- Postal and Shipping
  - 137M delivery sites

- Transportation
  - 120,000 miles of railroad
  - 590,000 highway bridges
  - 2M miles of pipeline
  - 300 ports

- Telecomm
  - 2B miles of cable
- Energy
  - 2,800 power plants
  - 300K production sites

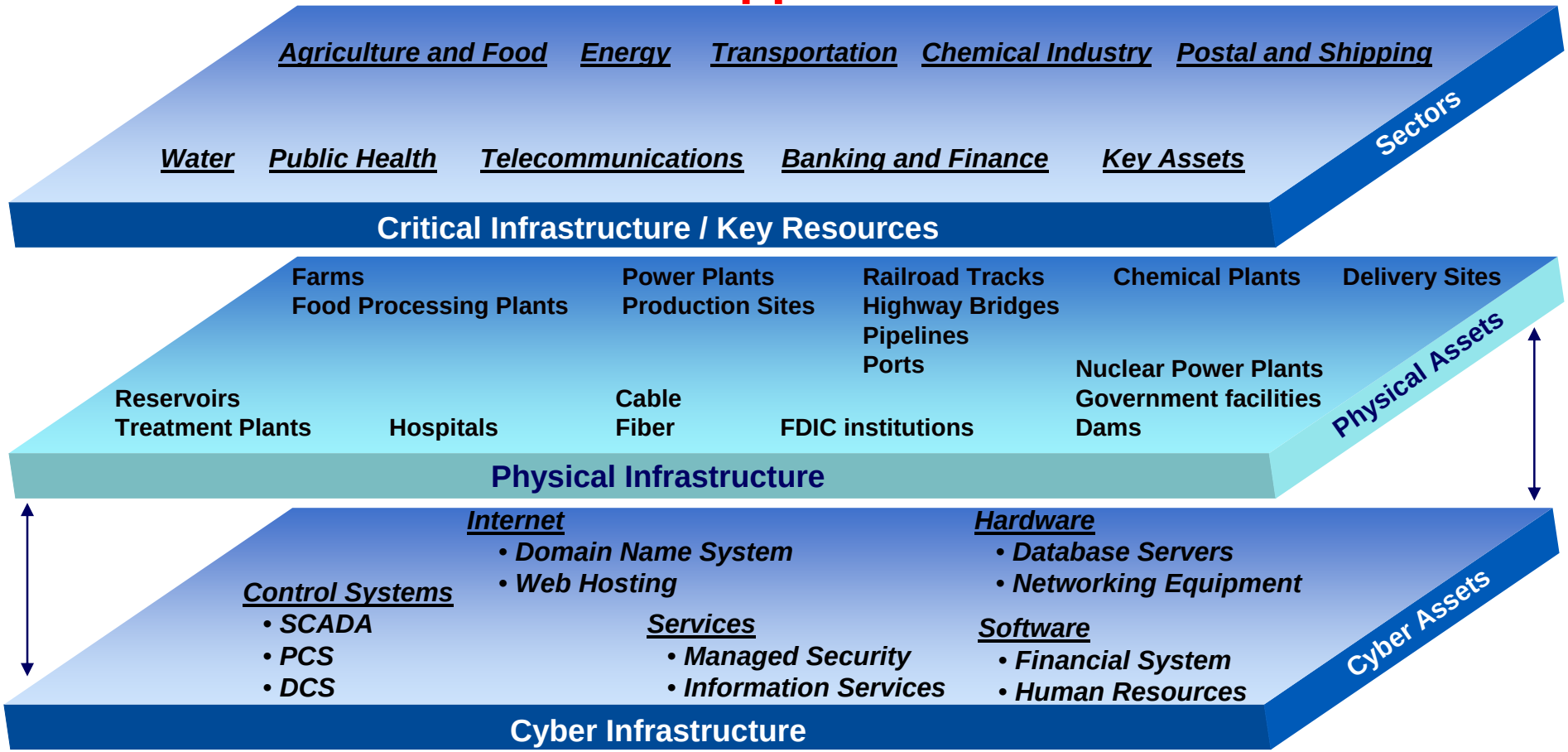
- Key Assets
  - 104 nuclear power plants
  - 80K dams
  - 5,800 historic buildings
  - 3,000 government facilities
  - commercial facilities / 460 skyscrapers

Homeland Security

An Asymmetric Target-rich Environment

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

Need for secure software applications



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

- Network disruptions lead to loss of:
  - Money
  - Time
  - Products
  - Reputation
  - Sensitive information
  - Potential loss of life through cascading effects on critical systems and infrastructure

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

Impact of Spyware not fully known

Needs in IT/Software Assurance

- **Software and IT vulnerabilities jeopardize infrastructure operations, business operations & services, intellectual property, and consumer trust**
- **Adversaries have capabilities to subvert the IT/software supply chain:**
  - Government and businesses rely on COTS products and commercial developers using foreign and non-vetted domestic suppliers to meet majority of IT requirements
  - Software & IT lifecycle processes offer opportunities to insert malicious code and to poorly design and build software which enables future exploitation
  - Off-shoring magnifies risks and creates new threats to security, business property and processes, and individuals' privacy – requires domestic strategies to mitigate those risks
- **Growing concern about inadequacies of suppliers' capabilities to build/deliver secure IT/software – too few practitioners with requisite knowledge and skills**
  - Current education & training provides too few practitioners with requisite competencies in secure software engineering – enrollment down in critical IT and software-related degree programs
  - Competition in higher-end skills is increasing – implications for individuals, companies, & countries
  - Concern about suppliers and practitioner not exercising "minimum level of responsible practice"
- **National-level focus needed to stay competitive in a global IT environment:**
  - Computing curriculum needs to evolve to better embrace changing nature of IT/software business
  - Educational policy and investment needed to foster innovation and increase IT-related enrollments
  - Improvements needed in the state-of-the-practice and state-of-the-art for IT & software capabilities
- **Processes and technologies are required to build trust into IT and software**

Strengthen operational resiliency

Shortage of IT/Software workforce with requisite skills

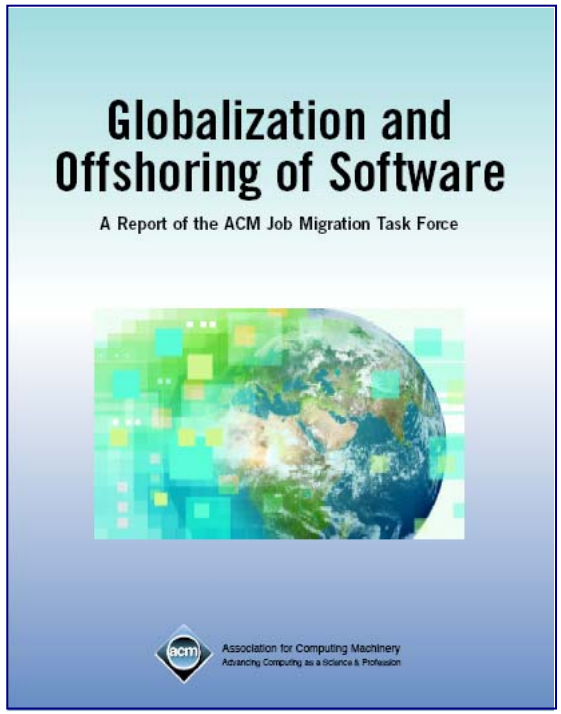
- **Current enrollment declines & shortages of IT/software professionals in the US partially driven by misperceptions of students and American public**
  - 2000 - 2003 trends indicated increase in US IT/software jobs being offshored/outsourced accompanied by rise in US unemployment – changed perceptions & career choices:
    - Perception – limited future in IT careers; jobs subject to offshoring/outsourcing
    - Response – declining enrollments in IT/computing/software engineering as students opt alternate disciplines
  - 2004 – 2006 trends indicate increase in domestic IT/software job positions
    - Offshoring continues, but domestic IT/software demands outpace offshoring
    - US employers cannot fill all positions with current IT/software domestic workforce.
- **Do schools provide relevant curriculum for students to be competitive in a global IT economy to enable requisite core competencies in IT/software?**
  - Computer programming easily outsourced/offshored; *
  - Domestic demand is high in IT/computing & information research, software engineering, systems analysts, network and systems administration, network and data communications analysts; *
  - Domestic demand raising in all aspects of cyber security and information assurance; increasing needs associated with software assurance.
- **Offshore sources sought, in part, to fill void of qualified US IT workforce**
  - Some companies now seeking to “back shore” jobs in US after offshoring presented unacceptable risks or lacked expected benefits
  - Some companies opt to offshore to access available IT/software workforce when functions can be outsourced with ROI and, in part, when jobs cannot be filled by US workforce with requisite skills

Homeland Security

** According to Catherine L Mann, Institute for International Economics, “Trade, Technology and Jobs,” Feb 2006*

Globalization and Offshoring of Software: 2006 Report of the ACM Job Migration Task Force

Provides the Emerging Trends, Debunked Myths, and More Realistic Picture of the Current State and Likely Future of IT



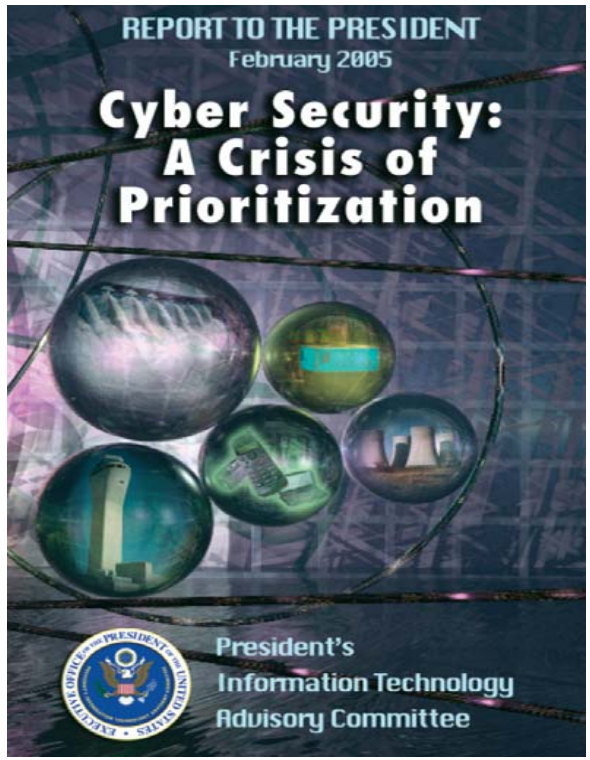
1. Offshoring: the Big Picture
2. Economics of Offshoring
3. The Country Perspective
4. Corporate Strategies for Software Globalization
5. Globalization of IT Research
6. Offshoring: Risks & Exposures
7. Education
8. Policies & Politics of Offshoring: An International Perspective

"Career opportunities in IT will remain strong in the countries where they have been strong in the past even as they grow in the countries that are targets of offshoring. The future, however, is one in which the individual will be situated in a more global competition. The brightness of the future for individuals, companies, or countries is centered on their ability to invest in building the foundations that foster innovation and invention."

http://www.acm.org/globalizationreport

PITAC* Findings Relative to Needs for Secure Software Engineering & Software Assurance

- Commercial software engineering today lacks the scientific underpinnings and rigorous controls needed to produce high-quality, secure products at acceptable cost.
- Commonly used software engineering practices permit dangerous errors, such as improper handling of buffer overflows, which enable hundreds of attack programs to compromise millions of computers every year.
- In the future, the Nation may face even more challenging problems as adversaries – both foreign and domestic – become increasingly sophisticated in their ability to insert malicious code into critical software.
- **Recommendations for increasing investment in cyber security provided to NITRD Interagency Working Group for Cyber Security & Information Assurance R&D**



* President's Information Technology Advisory Committee (PITAC) Report to the President, "Cyber Security: A Crisis of Prioritization," February 2005 identified top 10 areas in need of increased support, including: 'secure software engineering and software assurance' and 'metrics, benchmarks, and best practices' [Note: PITAC is now a part of PCAST]

Why Software Assurance is Critical

- Software is the core constituent of modern products and services – it enables functionality and business operations
- Dramatic increase in mission risk due to increasing:
  - Software dependence and system interdependence (weakest link syndrome)
  - Software Size & Complexity (obscures intent and precludes exhaustive test)
  - Outsourcing and use of un-vetted software supply chain (COTS & custom)
  - Attack sophistication (easing exploitation)
  - Reuse (unintended consequences increasing number of vulnerable targets)
  - Number of vulnerabilities & incidents with threats targeting software
  - Risk of Asymmetric Attack and Threats
- Increasing awareness and concern

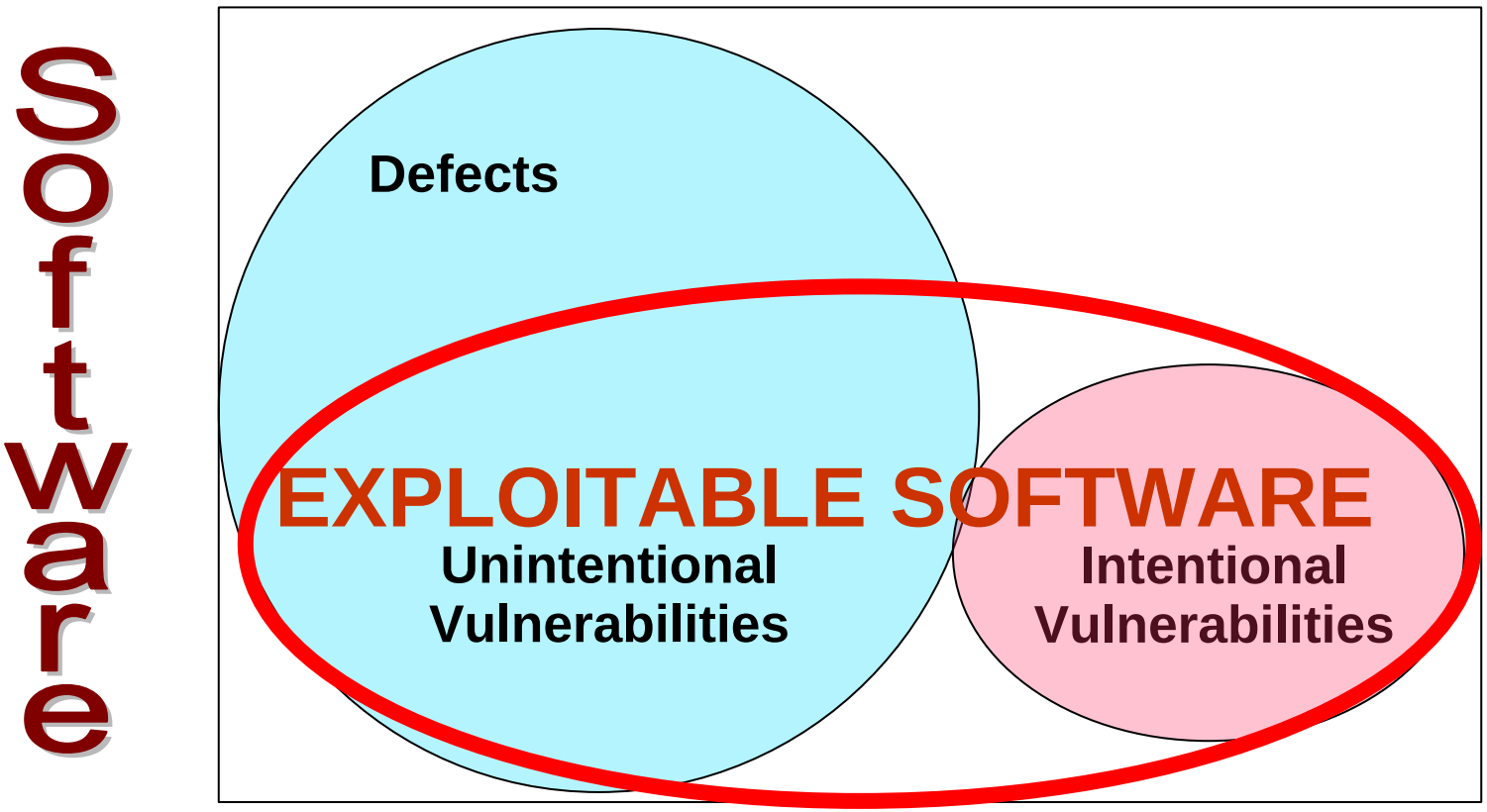
Software and the processes for acquiring and developing software represent a material weakness

Homeland Security

Software Assurance Addresses Exploitable Software:

Outcomes of non-secure practices and/or malicious intent

Exploitation potential of vulnerability is independent of "intent"



*Intentional vulnerabilities: spyware & malicious logic deliberately imbedded (might not be considered defects)

Homeland Security

Note: Chart is not to scale – notional representation -- for discussions

“Software Assurance”

Retrieved from "http://en.wikipedia.org/wiki/Software_Assurance"

Software Assurance (SwA) is: “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” — Source: Committee on National Security Systems (CNSS) Instruction No. 4009, “National Information Assurance Glossary”, Revised 2006 — http://www.cnss.gov/instructions.html

Alternate definitions:

[1] **Software Assurance (SwA)** relates to "the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software." - Source: DoD Software Assurance Initiative, 13 September 2005 - https://acc.dau.mil/CommunityBrowser.aspx?id=25749

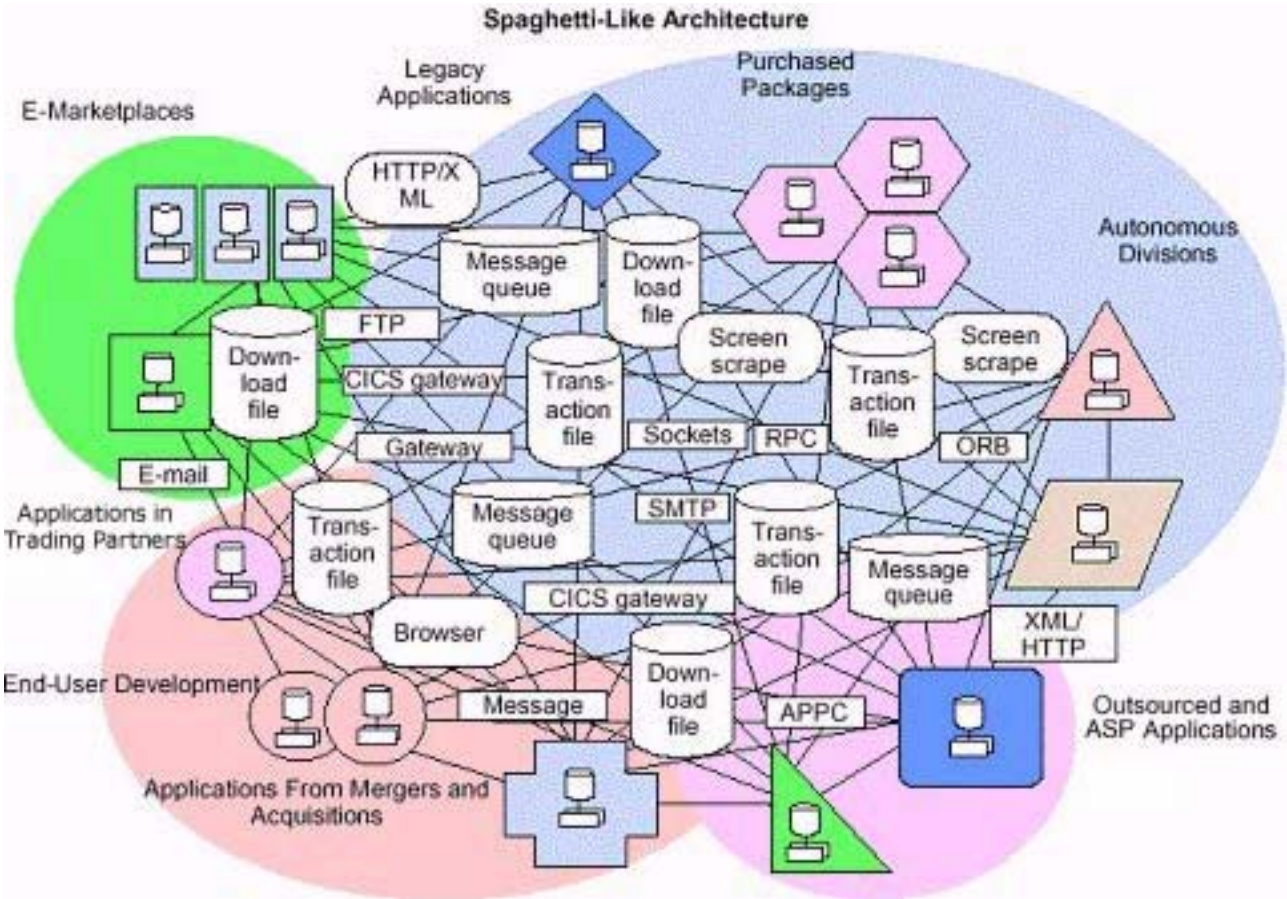
[2] **Software Assurance** - "Planned and systematic set of activities that ensures that software processes and products conform to requirements, standards, and procedures. It includes the disciplines of Quality Assurance, Quality Engineering, Verification and Validation, Nonconformance Reporting and Corrective Action, Safety Assurance, and Security Assurance and their application during a software life cycle." - Source: NASA-STD-2201-93 "Software Assurance Standard", 10 November 1992 - http://satc.gsfc.nasa.gov/assure/astd.txt

Software Assurance (SwA) is scoped to address:

- **Trustworthiness** - No exploitable vulnerabilities exist, either maliciously or intentionally inserted;
- **Predictable Execution** - Justifiable confidence that software, when executed, functions in a manner in which it is intended;
- **Conformance** - Planned and systematic set of multi-disciplinary activities that ensure software processes and products conform to requirements, standards/ procedures.

Software Assurance is a strategic initiative of the U.S. Department of Homeland Security to promote integrity, security, and reliability in software. The Program is 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 SwA "Build Security In" Portal

Reality of Existing Software



complex, multiple technologies with multiple suppliers

- Based on average defect rate, deployed software package of 1MLOCs has 6000 defects;
- if only 1% of those defects are security vulnerabilities, there are 60 different opportunities for hacker to attack the system

Homeland Security

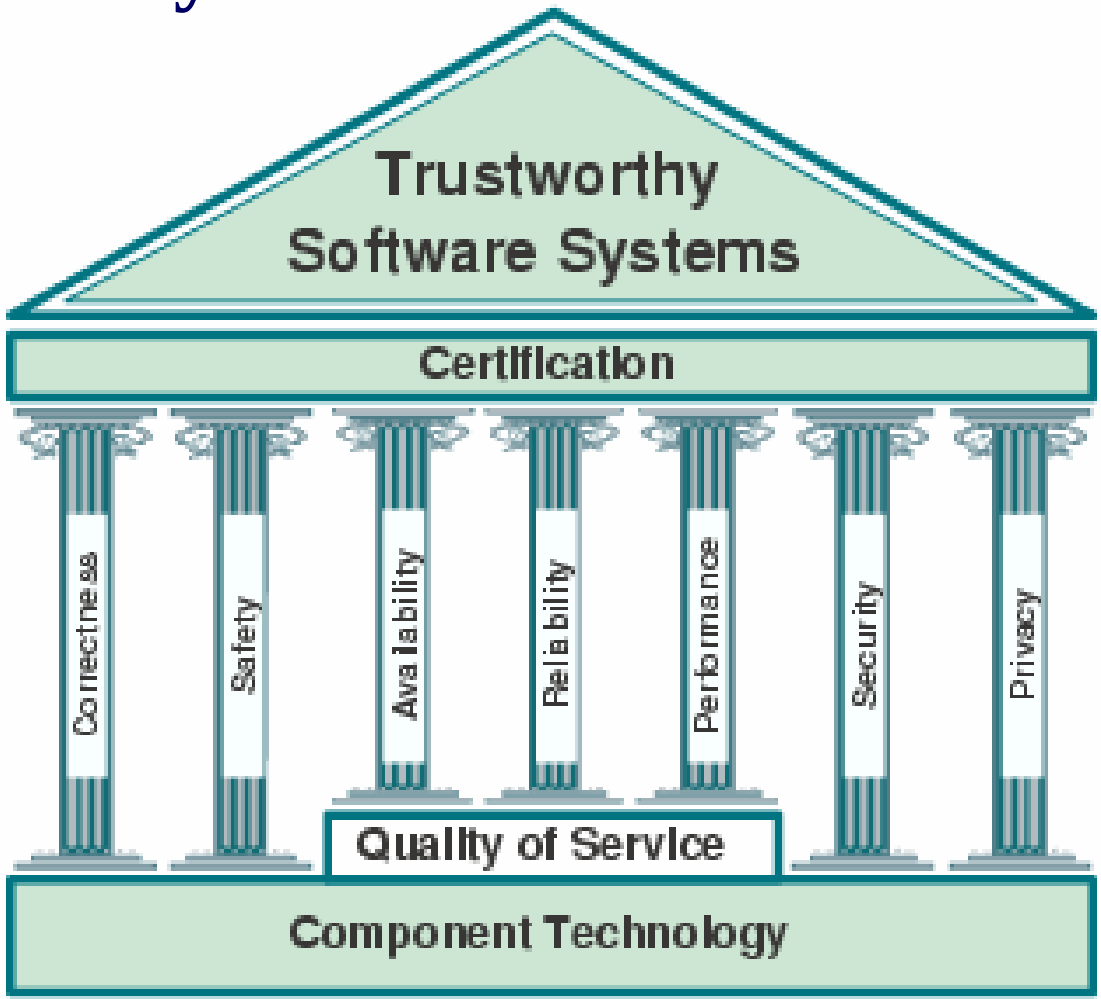
Gartner

Software Assurance contributes to Trustworthy Software Systems

Suppliers must consider enabling technologies and lifecycle processes

Holistic approach must factor in all relevant technologies, protection initiatives and contributing disciplines

Standards are required to better enable national and international commerce and to provide basis for certification



Homeland Security

Adopted from the TrustSoft Graduate School on Trustworthy Software Systems, started April 2005; funded by the German Research Foundation (DFG). See German Oldenburg http://trustsoft.uni-oldenburg.de

Software Assurance Comes From:

Knowing what it takes to "get" what we want

- Development/acquisition practices/process capabilities
- Criteria for assuring integrity & mitigating risks

Building and/or acquiring what we want

- Threat modeling and analysis
- Requirements engineering
- Failsafe design and defect-free code
- Supply Chain Management

Understanding what we built / acquired

- Production assurance evidence
- Comprehensive testing and diagnostics
- Formal methods & static analysis

*Multiple Sources:

DHS/NCSD, OASD(NII)IA, NSA, NASA, JHU/APL

Using what we understand

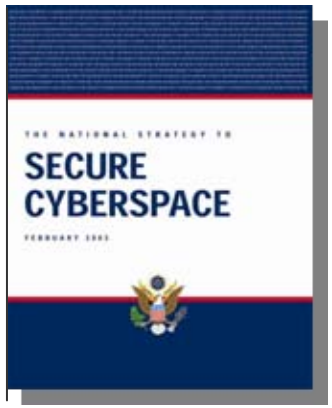
- Policy/practices for use & acquisition
- Composition of trust
- Hardware support

Homeland Security

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 in a manner in which it is intended
  - **Conformance** - Planned and systematic set of multi-disciplinary activities that ensure software processes and products conform to requirements, standards/ procedures

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

- Program framework encourages the production, evaluation and acquisition of better quality and more secure software; leverages resources to target the following four areas:
  - **People** – developers (includes education & training) 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** – software security improvements through specifications and guidelines for acquisition/outsourcing

Homeland Security

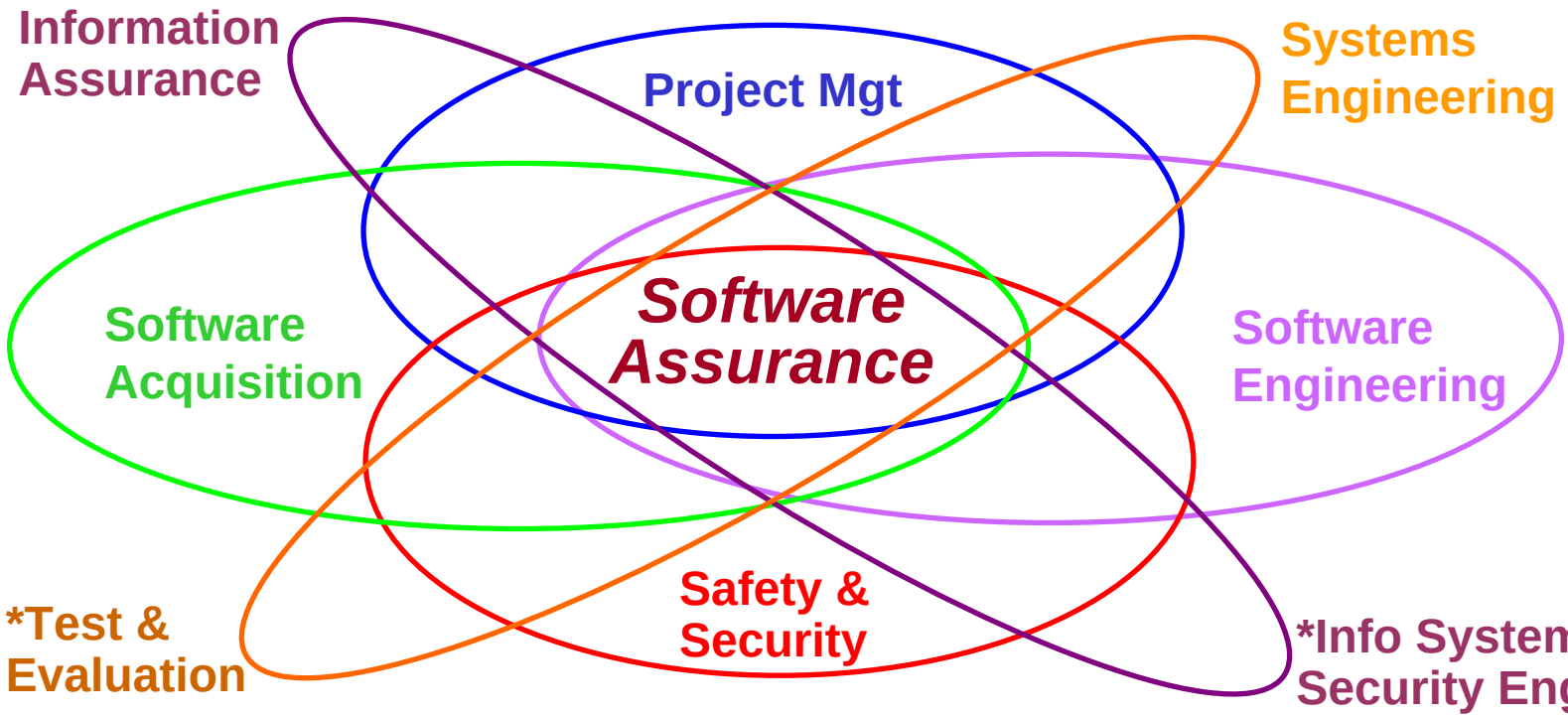
DHS Software Assurance: People

- Provide Guide to Software Assurance Common Body of Knowledge (CBK) as a framework to identify workforce needs for competencies and leverage standards and "best practices" to guide curriculum development for Software Assurance education and training**
  - Hosted Working Group sessions (April, June, Aug, & Oct 2005 and Jan, June & May 2006) with participation from academia, industry & Government
  - **Addressing three domains: "acquisition & supply," "development," and "post-release assurance" (sustainment)**
  - **Distribute CBK draft v1.0 in May 2006; next draft v1.1 in mid-July 2006**
  - After July 2006 draft, integrate other contributing "ilities" beyond "security"
  - Updating CBK awareness materials, including articles & FAQs
  - Update CBK -- identifying prioritization of practices and knowledge areas in domains, contributing disciplines and curricula, and "use" aids
  - Develop pilot training/education curriculum consistent with CBK in conjunction with early adopters for distribution by September 2007

Homeland Security

**NCSD Objective/Action 1.4.1

Disciplines Contributing to SwA CBK*



In Education and Training, Software Assurance could be addressed as:

- A “knowledge area” extension within each of the contributing disciplines;
- A stand-alone CBK drawing upon contributing disciplines;
- A set of functional roles, drawing upon a common body of knowledge; allowing more in-depth coverage dependent upon the specific roles.

Intent is to provide framework for curriculum development and evolution of contributing BOKs

Homeland Security

* See ‘Notes Page’ view for contributing BOK URLs and relevant links

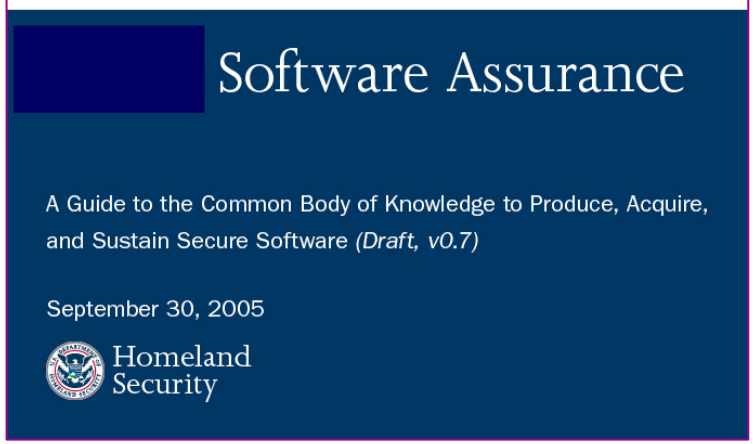
The intent is not to create a new profession of Software Assurance; rather, to provide a common body of knowledge: (1) from which to provide input for developing curriculum in related fields of study and (2) for evolving the contributing disciplines to better address the needs of software security, safety, dependability, reliability and integrity.

Software Assurance:
A Guide to the Common Body of Knowledge to Produce, Acquire and Sustain Secure Software, draft v1.0, May 2006

- Further review and comments have been solicited for feedback -- broader stakeholder community being contacted
- To provide comments, people have joined the Software Workforce Education and Training Working Group to collaborate through the US CERT Portal (https://us-cert.esportals.net/) using Organization ID 223
- **Version 0.9 released in Jan 2006 via Federal Register Notice, accessible via "**buildsecurityin.us-cert.gov**" with draft v1.0 released May 2006**
- Offered for informative use; it is not intended as a policy or a standard

Information for Educators & Trainers

(version 1.0 released May 2006)



Initial focus on "Secure Software"

Homeland Security

Software Assurance Common Body of Knowledge

General Changes throughout Document

- Concepts made consistent across CBK, *Security in the Software Lifecycle*, Acquisition Manager's Guide, and DHS SwA "Build Security In" web portal
- Definitions aligned with standard/common definitions (sources: NIST, ISO/IEC, CNSS, OWASP)
- "Government-centric" terms (e.g., "designated accrediting authority") replaced or augmented to accommodate needs of non-government audience
- Separated "functionality" from "assurance" and clarified relationships/distinctions:
  - Software security -vs- information security
  - Security properties of software -vs- security functions in software
  - Secure system engineering -vs- secure software development
- Reemphasized, clarified *software* security as document's initial focus;
- Providing structure to add other contributing "ilities" for software assurance (eg., safety, reliability, dependability, integrity)
- Added discussion of how some infosec functions can help ensure software security (e.g., process authentication)
- Moved detailed information security, security function discussions (e.g., identity management, cryptography) to appendices
- Added references to seminal works, highly-regarded recent works
- Provided other improvements to flow and clarity

Homeland Security

Software Assurance Common Body of Knowledge

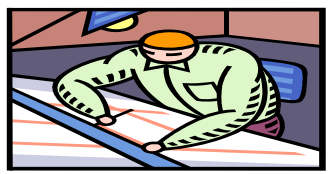
- **Changes to "Threats and Hazards" Section**
  - Focus on role vulnerable software plays in enabling exploits against *data*
  - Attack examples added from sectors other than National Security
  - Individual attack patterns descriptions replaced attack categories pointing to recognized sources of private and public sector attack/exploit data
  - Specific methods (e.g., STRIDE, SafSec) now presented as illustrative examples; alternatives to each identified
  - Distinctions between malware, surreptitious mechanisms (e.g., spyware), deception and redirection techniques (e.g., phishing) clarified
- **Key Changes in Other Sections**
  - Added discussion of "derived requirements" (usually non-operational)
  - Added discussion "negative" and "non-functional" requirements and their translation into requirements for functionality, functional parameters, or constraints on functionality
  - Accreditation discussion broadened to identify widely used commercial audit processes
  - Emphasized linkage between software reuse and acquisition considerations (security evaluation of *all* "reused" software, no matter how it is obtained)
  - Reorganized/enhanced discussion of secure software construction, including secure release; added discussion of "secure in deployment" considerations and techniques
  - Expanded, enhanced discussions of review and test techniques
  - Expanded categories of tools to add "safe" libraries, frameworks, IDEs, wrappers, testing tools, etc.

Reaching Relevant Stakeholders

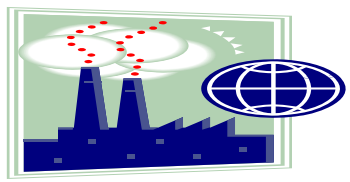
Leverage Evolving Efforts in Universities, Standards Organizations & Industry

Education	Professional Development	Training and Practices
• Curriculum • Accreditation Criteria	• Continuing Education • Certification	• Standards of Practice • Training programs
CNSS IA Courseware Eval	***Certified SW Development Professional (CSDP), IEEE***	***IEEE CS SW & Systems Engineering Standards Committee (S2ESC)***
IEEE/ACM SW Eng 2004 curriculum	***IEEE CSDP Prep Course***	***ISO/IEC JTC1/SC7 & SC27 and other committees***
AACSB & ABET	***IEEE CS SWE Book Series***	
AIS IS & MSIS curriculum		

University acceptance



Individual acceptance



Industry acceptance

Homeland Security

Adopted from "Integrating Software Engineering Standards" by IEEE Computer Society Liaison to ISO/IEC JTC 1/SC 7, James.W.Moore@ieee.org, 23 February 2005

SwA CBK relative to Computing Curricula

- Currently mapping SwA CBK content to Computing Curricula
- Goal is to provide the resulting mapping to assist in integrating SwA in relevant degree programs

Computing Curricula 2005

The Overview Report

covering undergraduate degree programs in
Computer Engineering
Computer Science
Information Systems
Information Technology
Software Engineering

A volume of the *Computing Curricula Series*

The Joint Task Force for Computing Curricula 2005

A cooperative project of
The Association for Computing Machinery (ACM)
The Association for Information Systems (AIS)
The Computer Society (IEEE-CS)

30 September 2005

Homeland Security

DHS Software Assurance: Process

- Provide practical guidance in software assurance practices and process improvement methodologies**
  - Launched a web-based repository “Build Security In” on US-CERT web site “**buildsecurityin.us-cert.gov** on October 3, 2005
  - Publishing developers’ guide “SECURING THE SOFTWARE LIFECYCLE”
  - Developing business case analysis to support software security throughout lifecycle practices
  - Completing DHS/DoD co-sponsored comprehensive review of the NIAP & use of the Common Criteria
  - Continuing to seek broader participation of relevant stakeholder organizations and professional societies
  - Participate in relevant standards bodies; identify software assurance gaps in applicable standards from ISO/IEC, IEEE, NIST, ANSI, OMG, CNSS, and Open Group and support effort through DHS-sponsored SwA Processes and Practices Working group

Homeland Security

**NCSD Goal/Action 1.4.2

DHS Software Assurance: Process (cont.)

- Provide practical guidance in software assurance practices and process improvement methodologies**
  - Launched a web-based central repository "Build Security In" on US-CERT web site https://**buildsecurityin.us-cert.gov** on October 3, 2005

– Provides dissemination of recommended "sound" practices and technologies for secure software development

– Continuing to sponsor work with CMU Software Engineering Institute and industry to further develop practical guidance and update the web-based repository

  - Updating site to include additional development guidance and add new focus for acquisition and ops/sustainment

Homeland Security

**NCSD Objective/Action 1.4.2

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

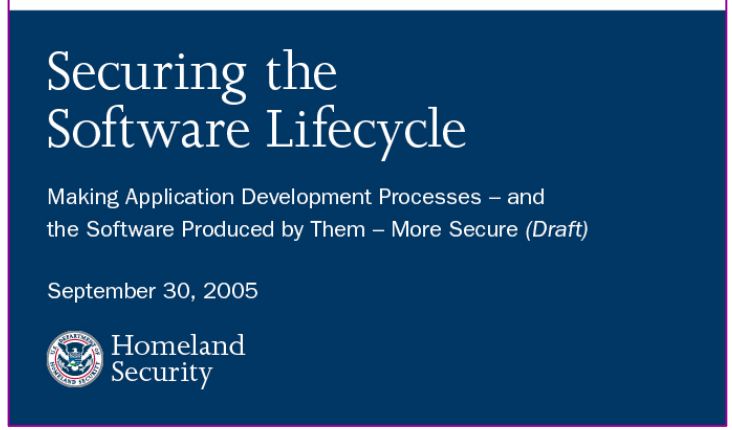
Homeland Security

"Securing the Software Lifecycle: Making Application Development Processes – and the Software Produced by Them – More Secure"

- Initial content from DoD-sponsored *Application Security Developer Guides*:
  - Securing the Software Development Lifecycle
  - Security Requirements Engineering Methodology
  - Reference Set of Application Security Requirements
  - Secure Design, Implementation, and Deployment
  - Secure Assembly of Software Components
  - Secure Use of C and C++
  - Secure Use of Java-Based Technologies
  - Software Security Testing
- Content updated, expanded, & revised based on documents and inputs from other sources across SwA community

Information for Developers

(version 1.0 released April 2006)



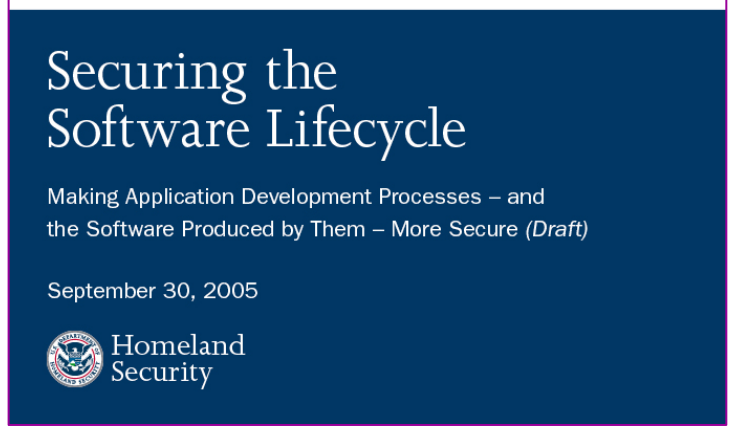
Homeland Security

"Securing the Software Lifecycle:
Making Application Development Processes – and the Software Produced by Them – More Secure"

- Offered for informative use; it is not intended as a policy or standard
  - Further review and comments have been solicited for feedback -- broader stakeholder community being contacted
  - Previously, to provide comments, people joined the Software Processes and Practices WG to collaborate through US CERT Portal (https://us-cert.esportals.net/) using Organization ID 223
- **Latest draft version released Jan 2006 via Federal Register Notice, accessible via** "buildsecurityin.us-cert.gov" **with draft v1.0 released April 2006**

Information for Developers

(version 1.0 released April 2006)



Homeland Security

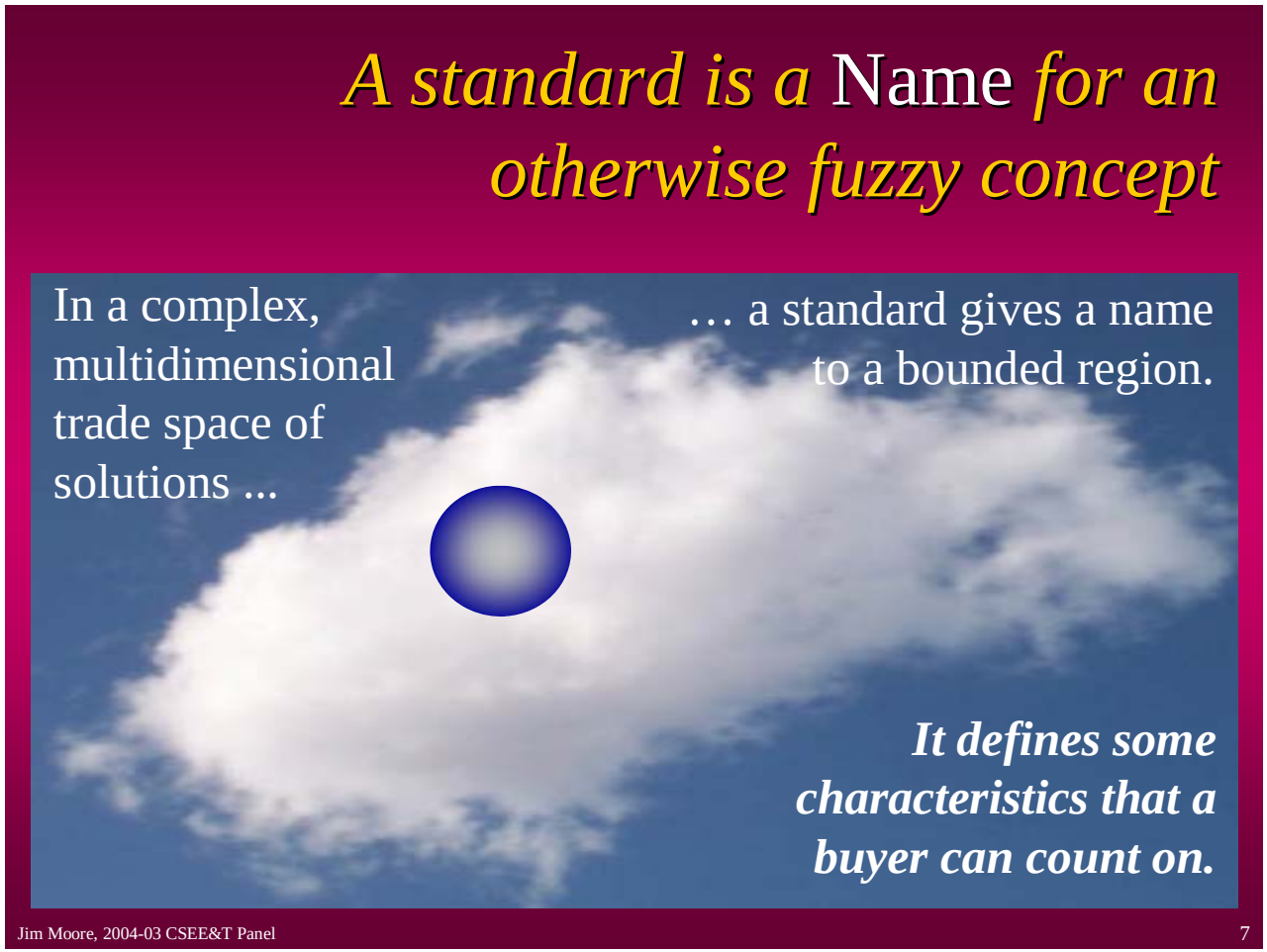
DHS Software Assurance: Process (cont.)

- Provide practical guidance in software assurance process improvement methodologies** (cont.)
  - Participate in relevant standards bodies;
  - identify software assurance gaps in applicable standards from:
    - ISO/IEC,
    - IEEE,
    - NIST,
    - ANSI,
    - OMG,
    - CNSS, and
    - Open Group
- Support effort through DHS-sponsored SwA Processes and Practices Working group
  - April, June, August, October, and Nov-Dec 2005
  - January, March, May, Aug and Oct 2006

Homeland Security

**NCSD Objective/Action 1.4.2

Value of Standards



- ***Software Assurance*** **needs standards to assign names to practices or collections of practices.**
- **This enables communication between:**
  - **Buyer and seller**
  - **Government and industry**
  - **Insurer and insured**

Standards represent the "minimum level of responsible practice" and "sound practices" that are consensus-based, not necessarily the best available methods

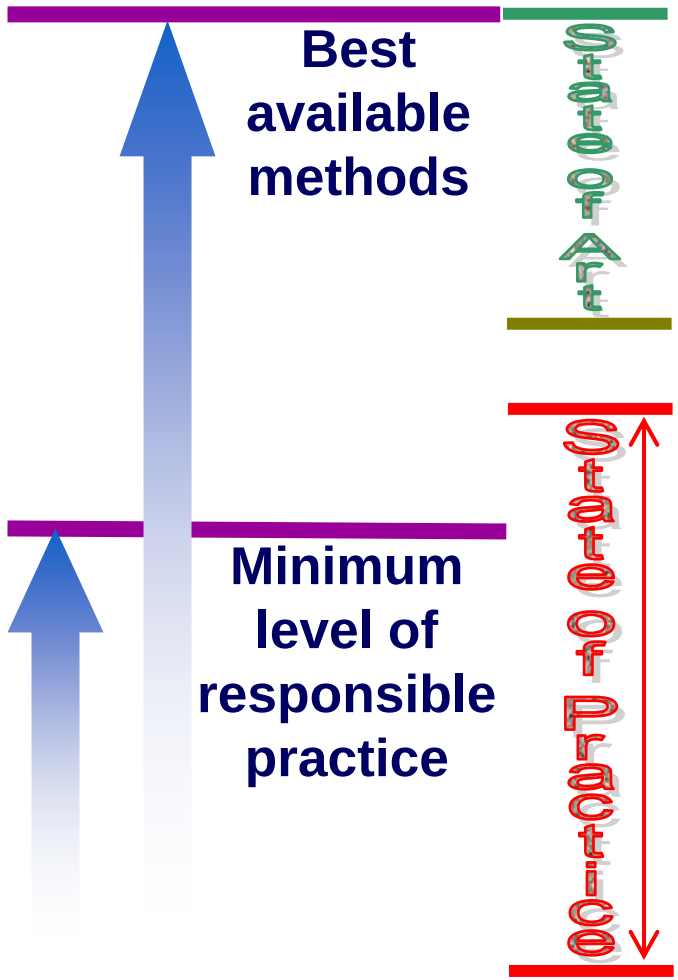
Using Standards and Best Practices to Close gaps between state-of-the-practice and state-of-the-art *1, 2

Raising the Ceiling

- *Information Assurance, Cyber Security* and *System Safety* typically treat the concerns of the most critical system assets.
  - They prescribe extra practices (and possibly, extra effort) in developing, sustaining and operating such systems.

Raising the Floor

- However, *some* of the concerns of *Software Assurance* involve simple things that any user or developer should do.
  - They don't increase lifecycle costs.
  - In many cases, they just specify "stop making avoidable mistakes."



*[1] Adopted from Software Assurance briefing on "ISO Harmonization of Standardized Software and System Life Cycle Processes," by Jim Moore, MITRE, June 2, 2005, *[2] US 2nd National Software Summit, April 29, 2005 Report (see http://www.cnsoftware.org) identified major gaps in requirements for software tools and technologies to routinely develop error-free software and the state-of-the-art and gaps in state-of-the-art and state-of-the-practice

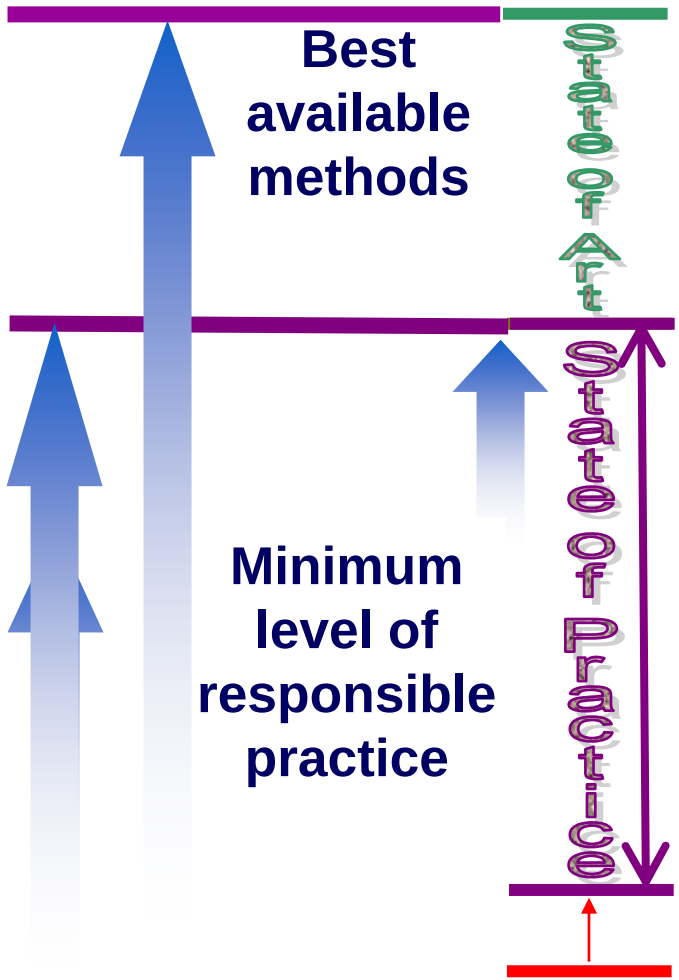
Using Standards and Best Practices to Close gaps between state-of-the-practice and state-of-the-art *1, 2

Raising the Ceiling

- *Information Assurance, Cyber Security* and *System Safety* typically treat the concerns of the most critical system assets.
  - They prescribe extra practices (and possibly, extra effort) in developing, sustaining and operating such systems.

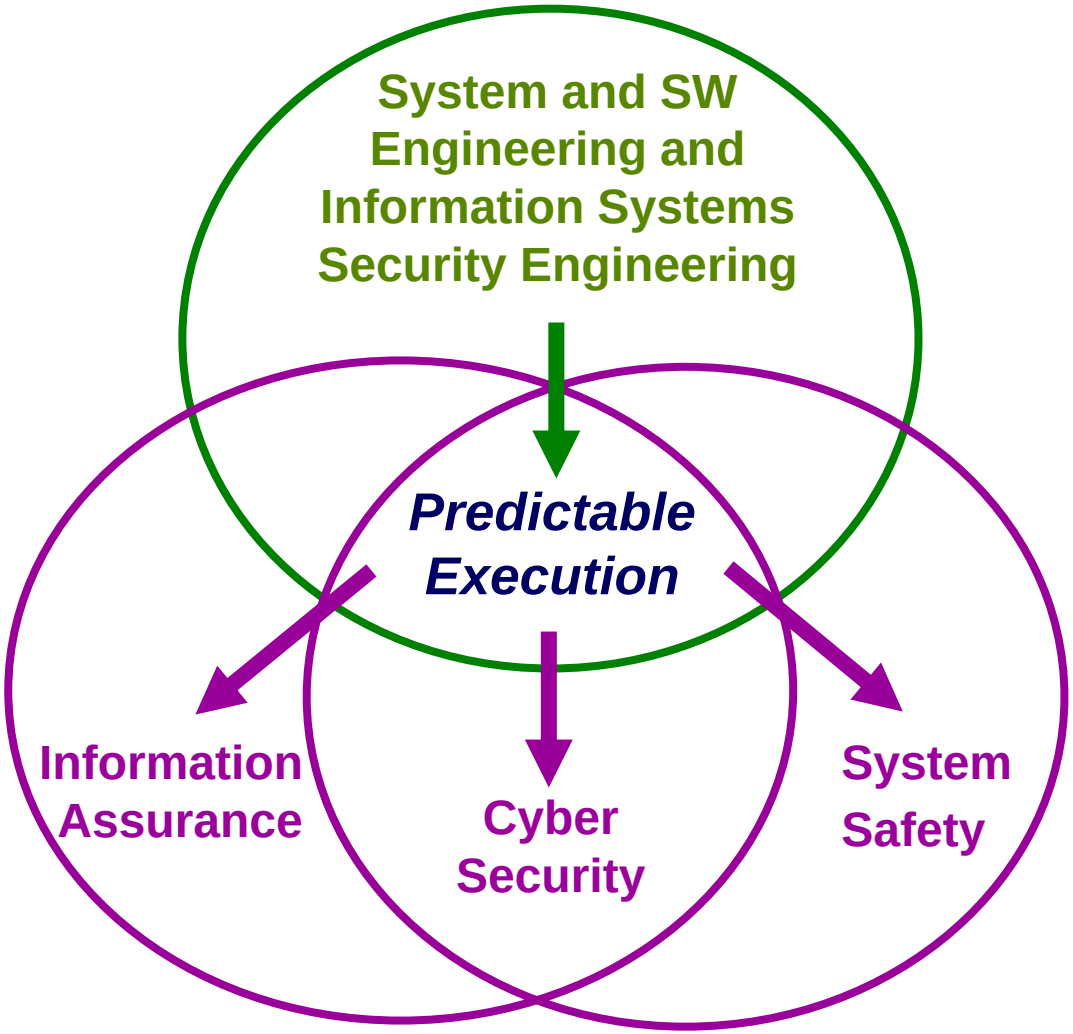
Raising the Floor

- However, *some* of the concerns of *Software Assurance* involve simple things that any user or developer should do.
  - They don't increase lifecycle costs.
  - In many cases, they just specify "stop making avoidable mistakes."



*[1] Adopted from Software Assurance briefing on "ISO Harmonization of Standardized Software and System Life Cycle Processes," by Jim Moore, MITRE, June 2, 2005, *[2] US 2nd National Software Summit, April 29, 2005 Report (see http://www.cnsoftware.org) identified major gaps in requirements for software tools and technologies to routinely develop error-free software and the state-of-the-art and gaps in state-of-the-art and state-of-the-practice

Relating SW Assurance to Engineering Disciplines



For a safety/security analysis to be valid …

The execution of the system must be *predictable*.

This requires …

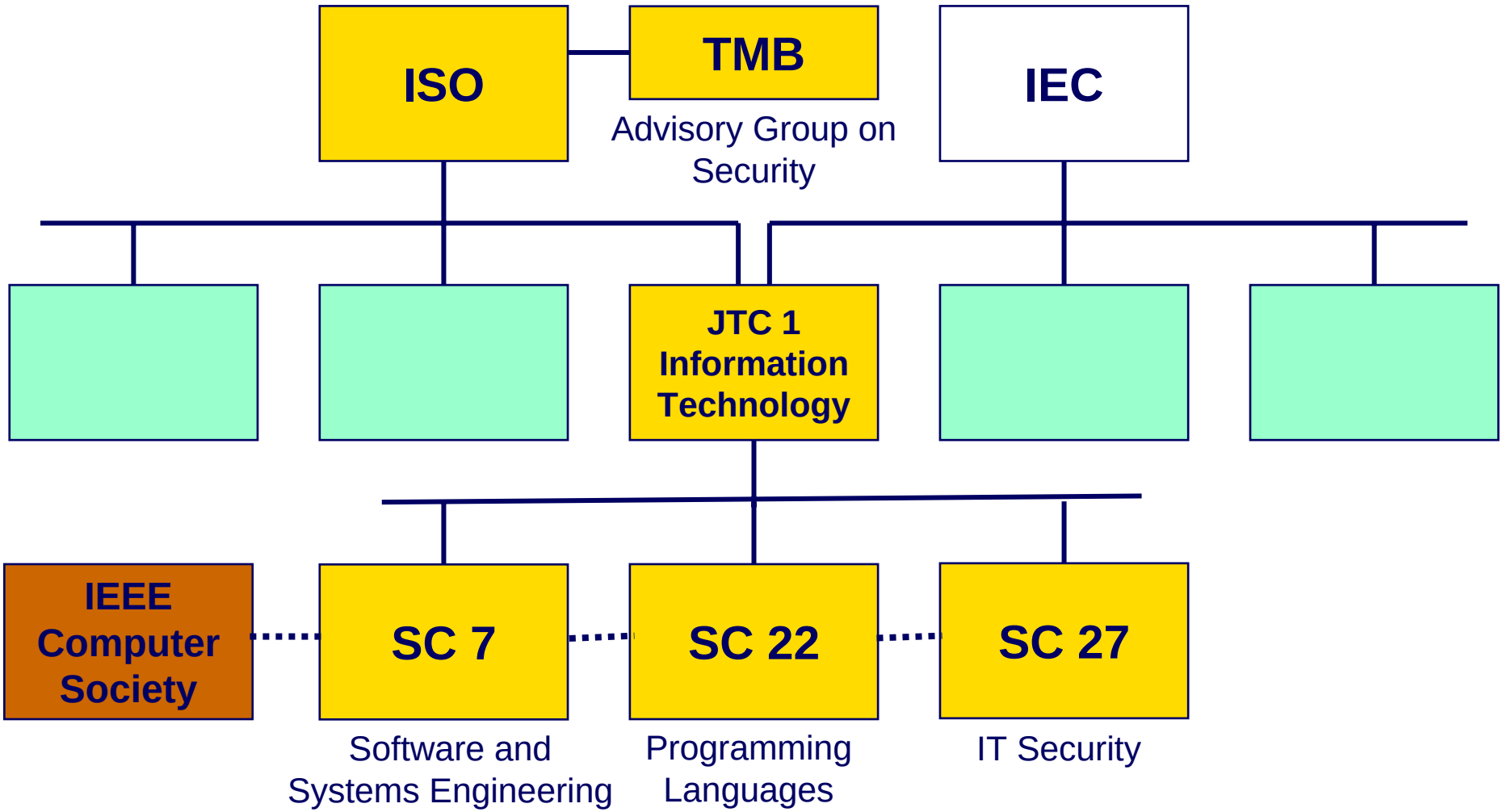
- **Correct implementation of requirements, expectations and regulations.** } ***Traditional concern***
- **Exclusion of unwanted function even in the face of attempted exploitation.** } ***Growing concern***

Homeland Security

Predictable Execution = requisite enabling characteristic

*Adopted from Jim Moore, IEEE CS S2ESC Liaison to ISO SC7

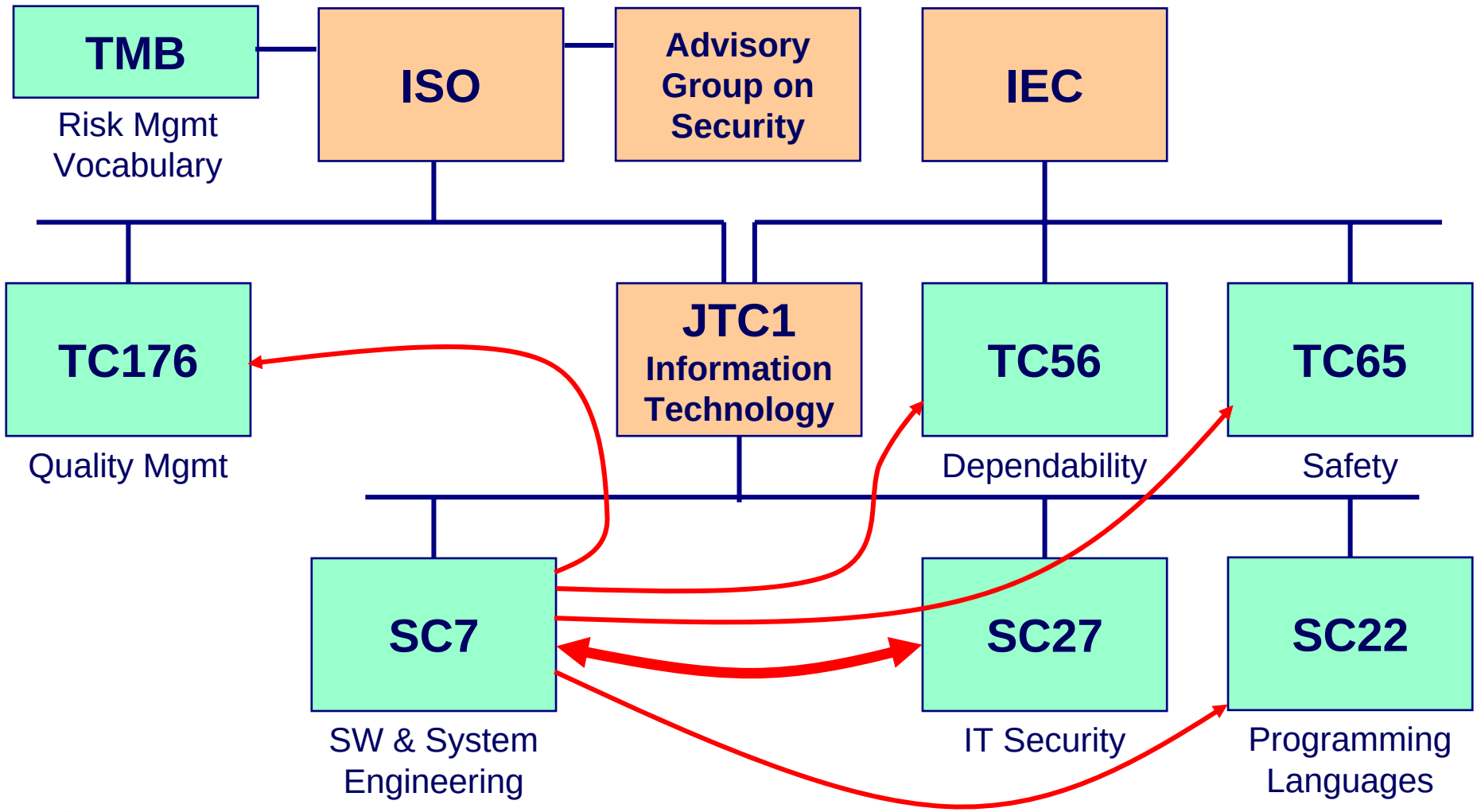
Security and Assurance Concerns in ISO



Homeland Security

Liaison role between IEEE CS S2ESC and between ISO SCs

SwA Concerns of Standards Organizations



Homeland Security

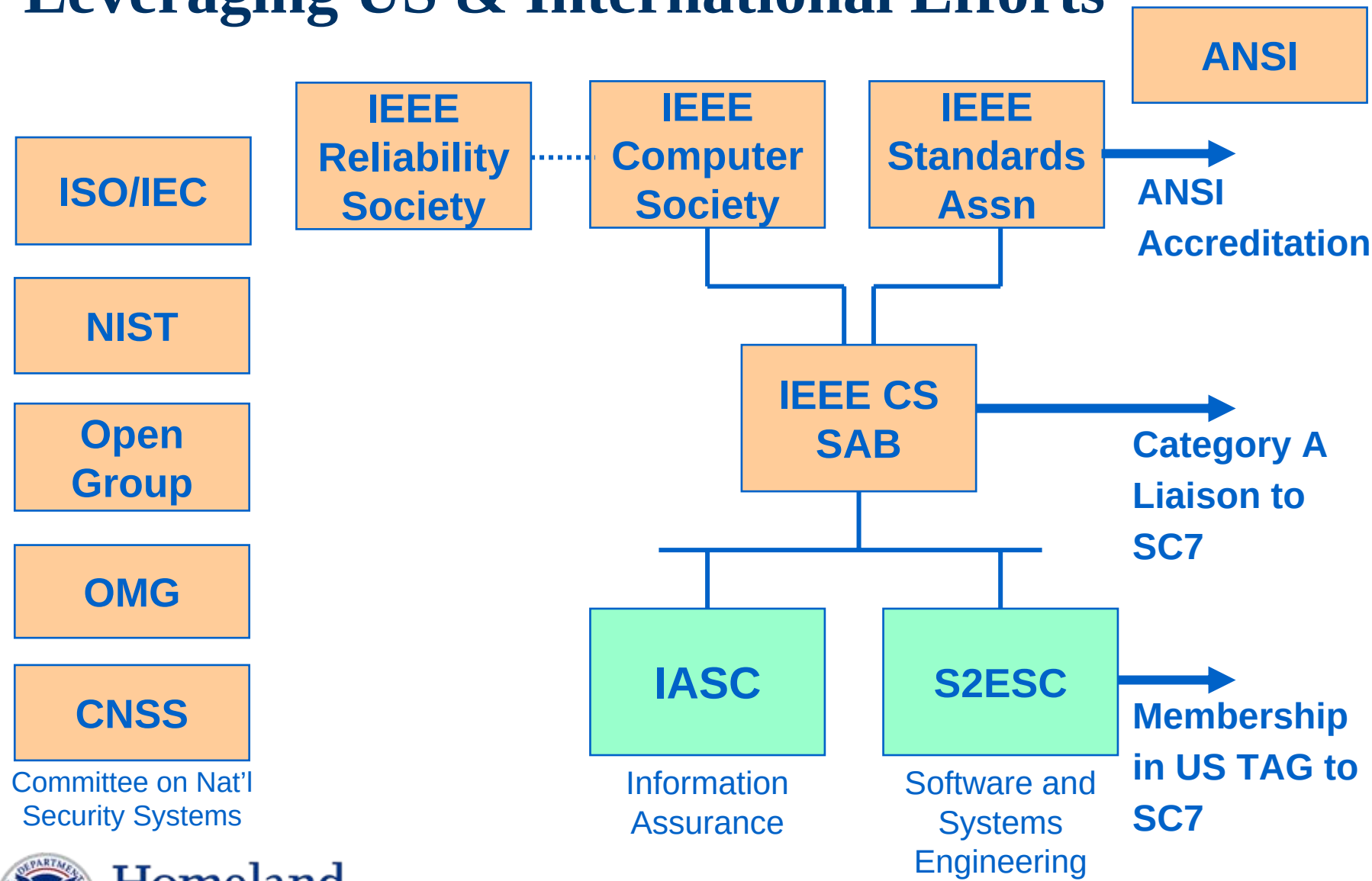
* DHS NCSD has membership on SC7, SC27 & IEEE S2ESC leveraging Liaisons in place or requested with other committees

ISO SC27 (INCITS CS1) Standards Portfolio

- Management
  - Information security and systems
  - Third party information security service providers (outsourcing)
- Measurement and Assessment
  - Security Metrics
  - Security Checklists
  - IT security assessment of operational systems
  - IT security evaluation and assurance
- IA & Cyber Security Requirements and Operations
  - Protection Profiles
  - Security requirements for cryptographic modules
  - Intrusion detection
  - Network security
  - Incident handling
  - Role based access control

Homeland Security

Leveraging US & International Efforts



Homeland Security

Scope of ISO/IEC 15026 “System and Software Assurance”

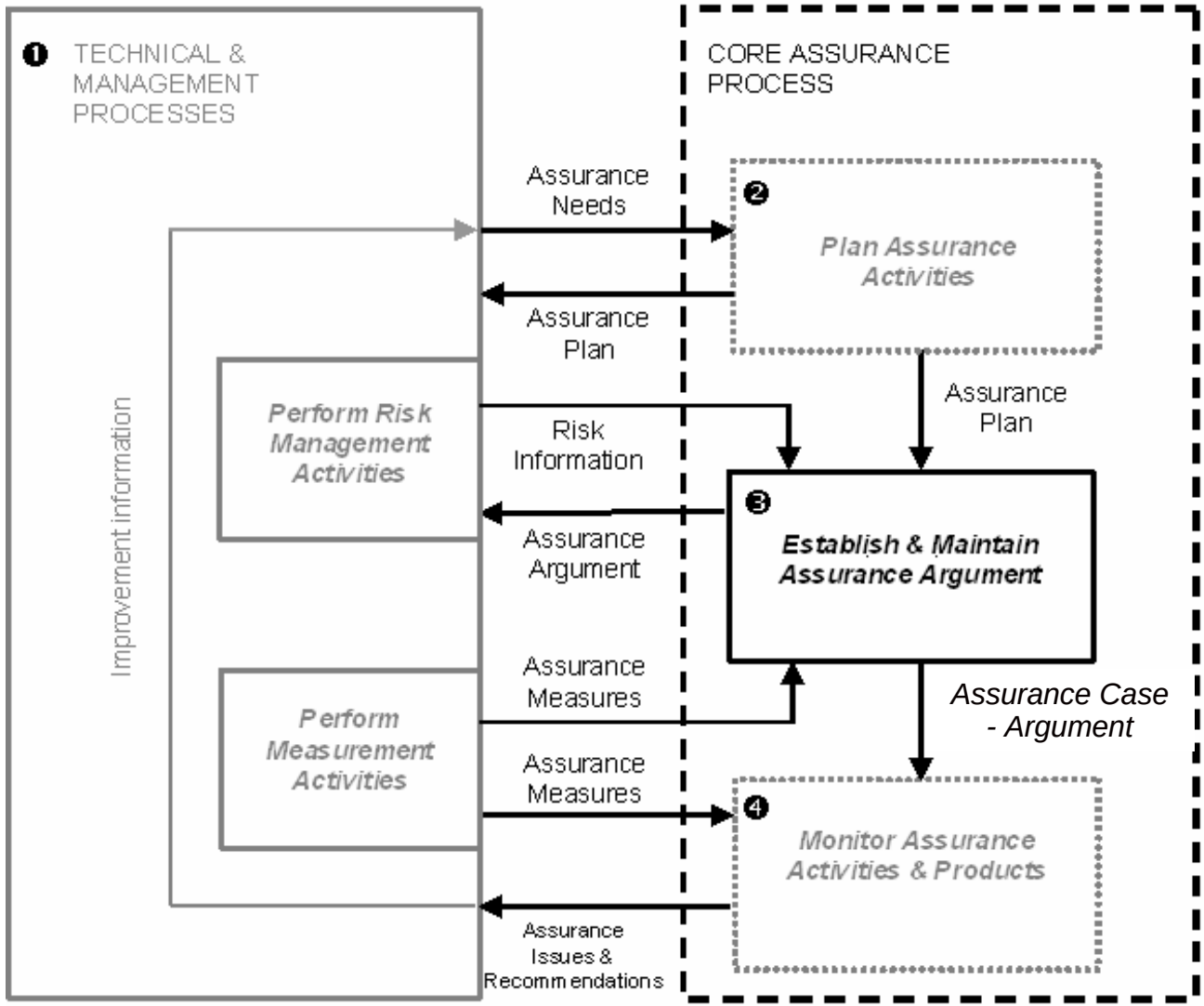
“System and software assurance focuses on the management of risk and assurance of safety, security, and dependability within the context of system and software life cycles.”

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

Adopted from Paul Croll’s SSTC May 2005 presentation, “Best Practices for Delivering Safe, Secure, and Dependable Mission Capabilities”

ISO/IEC 15026 – 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 Metrics
- Establishes centrality of the Assurance Argument
- Leverages IT security concepts and terminology in ISO/IEC15443
- Leverages OMG's ADM Task Force – Knowledge Discovery Meta-model



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

The Assurance Case/Argument

Structure

Part 1: A coherent argument for the safety and security of the product or service

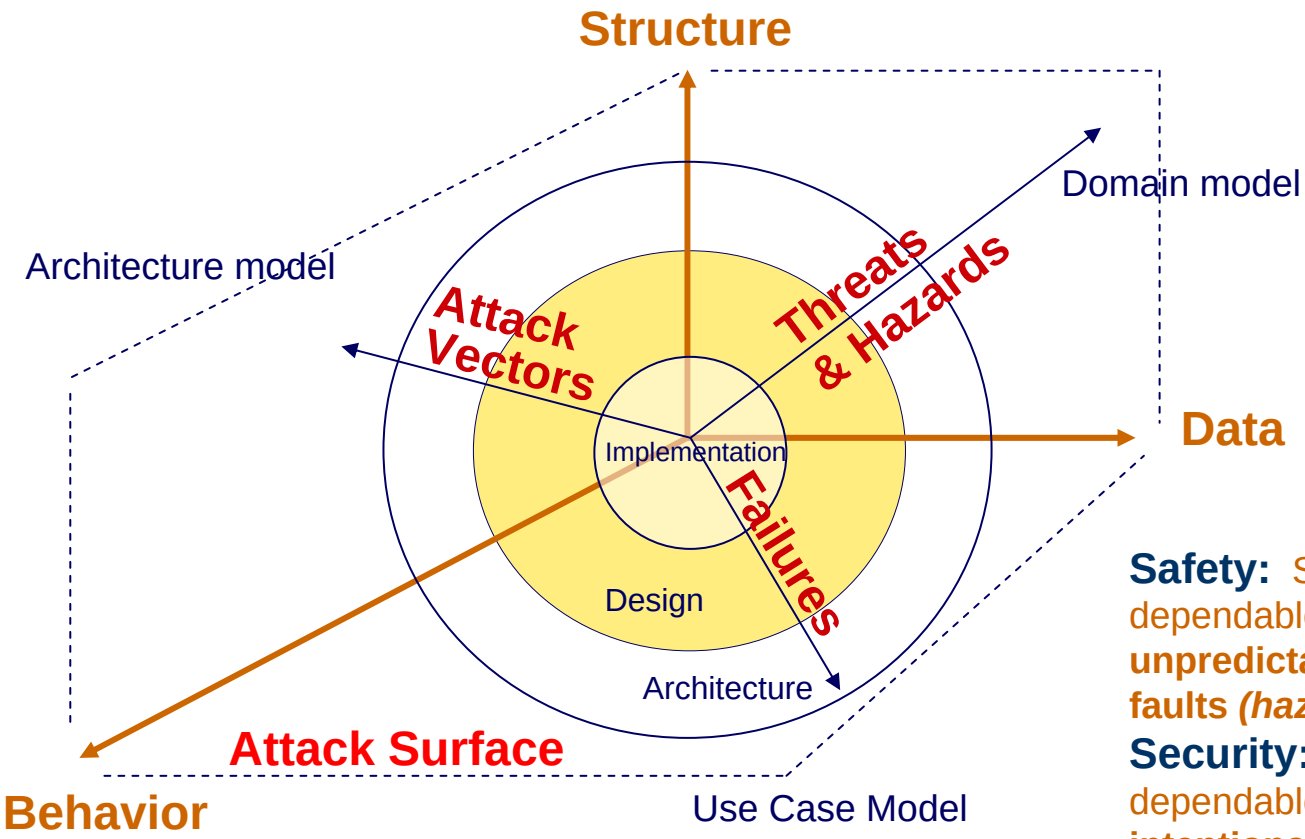
Part 2: A set of supporting evidence
…
…

Attributes

- ❑ Clear
- ❑ Consistent
- ❑ Complete
- ❑ Comprehensible
- ❑ Defensible
- ❑ Bounded
- ❑ Addresses all life cycle stages

*Adopted from Paul Croll, ISO SC7 WG9 Editor for Systems and Software Assurance

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 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

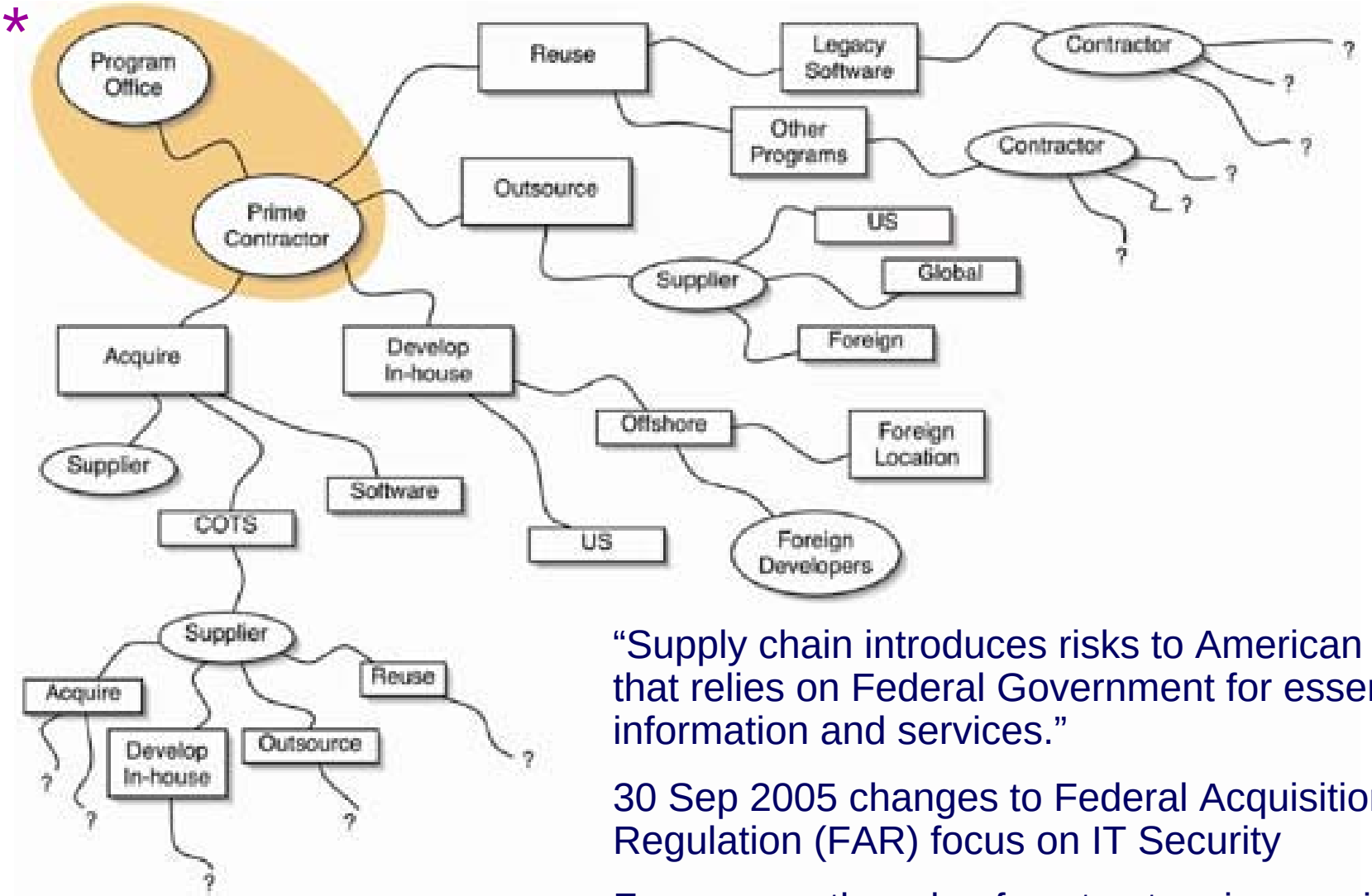
DHS Software Assurance: Acquisition

- **Collaborate with stakeholders to enhance software supply chain management through improved risk mitigation and contracting for secure software ****
  - Collaborate with stakeholder organizations to support acquisition community to develop and disseminate:
    - Due-diligence questionnaire for RFI/RFP and source selection decision-making
    - Templates and sample statement of work / procurement language for acquisition and evaluation based on successful models
    - Acquisition Managers guidebook on acquisition/procurement of secure software-intensive systems and services
  - Collaborate with government and industry working groups to:
    - Identify needs for reducing risks associated with software supply chain
    - Provide acquisition training and education to develop applicable curriculum
  - Chair IEEE CS S2ESC WG to update of IEEE 1062, “Software Acquisition”
  - Collaborate with agencies implementing changes responsive to changes in the FAR that incorporated IT security provisions of FISMA when buying goods and services

Homeland Security

**NCSD Objective/Action 1.4.4

*



"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"

FISMA IT security provisions now in FAR

- 30 Sep 2005 amended FAR parts 1, 2, 7, 11, and 39 implements IT security provisions of FISMA for all phases of IT acquisition life cycle
  - Incorporates FISMA (Federal Information Systems Management Act) into Federal Acquisition with clear and consistent IT security guidance
    - Require agencies to identify and provide InfoSec protections commensurate with security risks to Federal information collected or maintained for the agency and info systems used or operated on behalf of an agency by a contractor
    - Incorporate IT security in buying goods and services
    - Require adherence to Federal Information Processing Standards
    - Require agency security policy and requirements in IT acquisitions
    - Require contractors and Fed employees be subjected to same requirements in accessing Fed IT systems and data
  - Applies Information Assurance definitions for Integrity, Confidentiality and Availability to Federal IT, including Sensitive But Unclassified information

Homeland Security

See www.regulations.gov and article at www.fcw.com/article90982-09-30-05-Web

NIST Enterprise Risk Management Framework

FIPS 199 / SP 800-60

Starting Point

Security Categorization

Defines category of information system according to potential impact of loss

SP 800-53 / FIPS 200

Security Control Selection

Selects minimum security controls (i.e., safeguards and countermeasures) planned or in place to protect the information system

SP 800-37

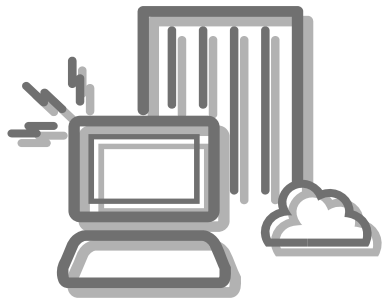
Security Control Monitoring

Continuously tracks changes to the information system that may affect security controls and assesses control effectiveness

SP 800-53 / FIPS 200 / SP 800-30

Security Control Refinement

Uses risk assessment to adjust minimum control set based on local conditions, required threat coverage, and specific agency requirements



SP 800-37

System Authorization

Determines risk to agency operations, agency assets, or individuals and, if acceptable, authorizes information system processing

SP 800-18

Security Control Documentation

In system security plan, provides a an overview of the security requirements for the information system and documents the security controls planned or in place

SP 800-70

Security Control Implementation

Implements security controls in new or legacy information systems; implements security configuration checklists

SP 800-53A / SP 800-37

Security Control Assessment

Determines extent to which the security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements

Homeland Security

Source: FISMA Implementation Project, Dr. Ron Ross, NIST, April 2004

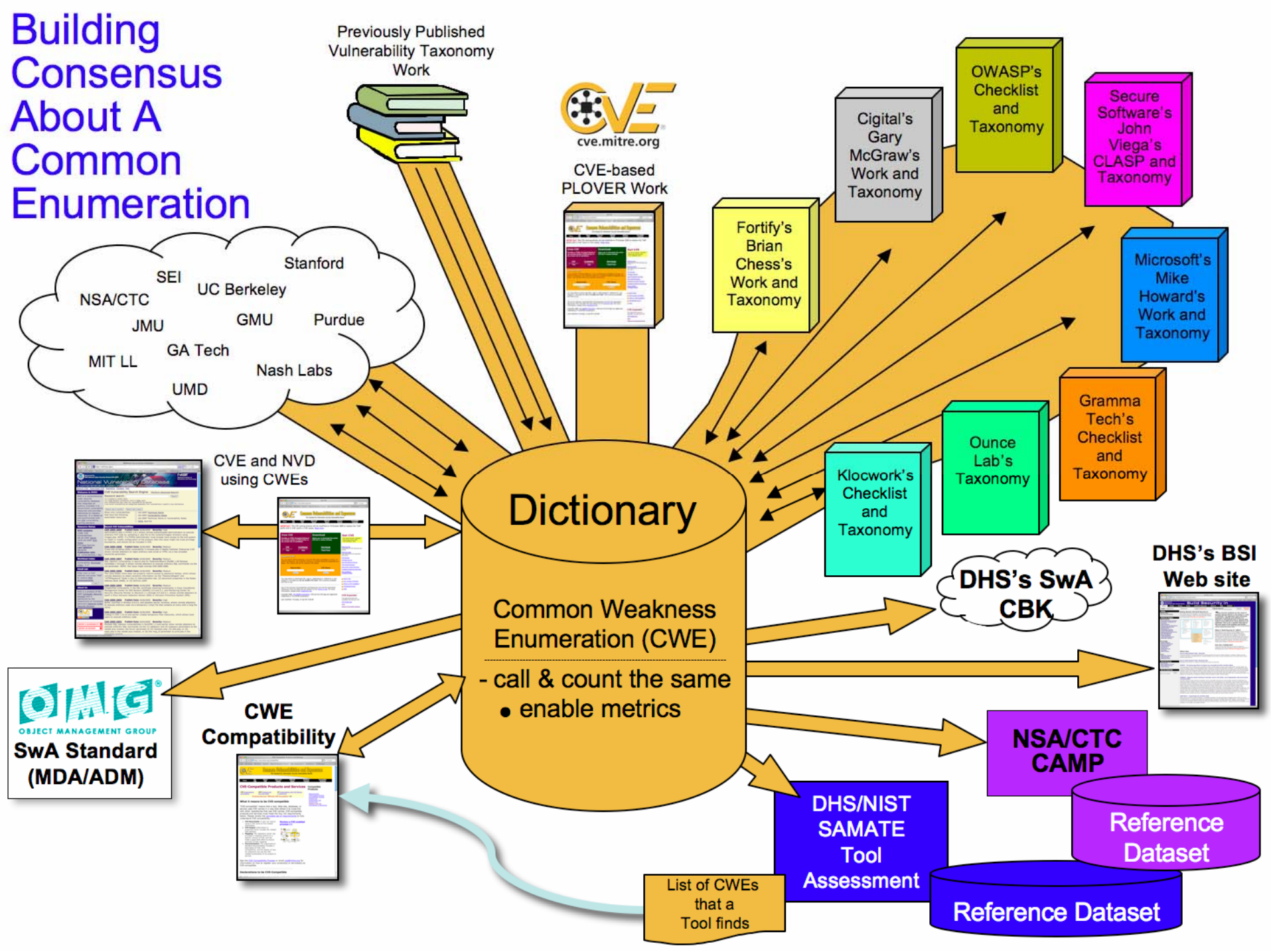
DHS Software Assurance: Technology

- Enhance software security measurement, advocate SwA R&D, and assess SwA testing and diagnostic tools**
  - Collaborate with NIST to inventory SwA tools; measure effectiveness, identify gaps and conflicts, and develop a plan to eliminate gaps and conflicts
    - NIST SAMATE workshops to assess, measure, and validate tool effectiveness
    - DHS NCSD sponsored work provides common taxonomy to compare capabilities
    - DHS NCSD task provides common attack pattern enumeration and classification
  - Collaborate with other agencies and allied organizations to:
    - Enhance “software security measurement” to support SwA requirements and support decision-making for measuring risk exposure
    - Explore needs and organizing mechanisms for federated labs
  - Identify SwA R&D requirements for DHS S&T and multi-agency TSWG; coordinating requirements and priorities with other federal agencies
    - Advocate SwA R&D priorities through DHS S&T Directorate and multi-agency Technical Support Working Group
    - Update R&D needs & priorities specific for SwA (list available)
    - Contribute to multi-agency Cyber Security and IA R&D provided to stakeholders.

Homeland Security

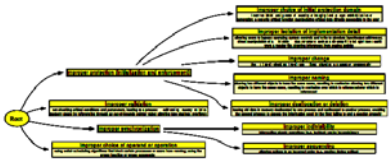
**NCSD Objective/Action 1.4.3

Building Consensus About A Common Enumeration



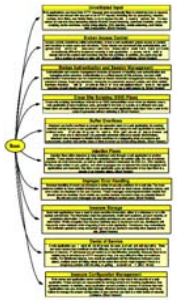
Taxonomies Contributing to Common Flaw Enumeration

Protection Analysis

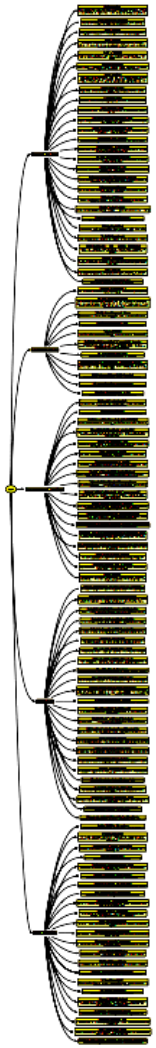


Weber

OWASP



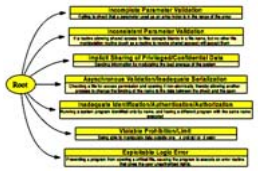
CLASP



Microsoft

PLOVER

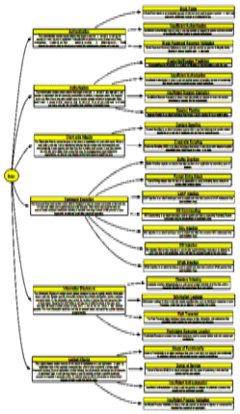
RISOS



Bishop

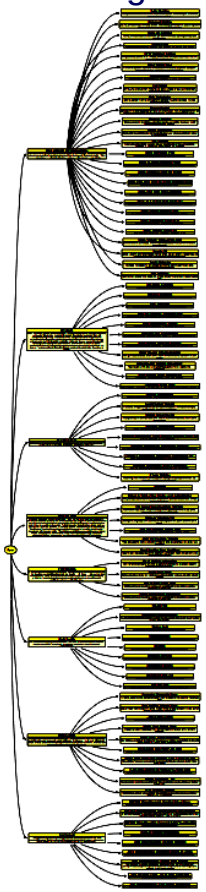
Aslam

WASC

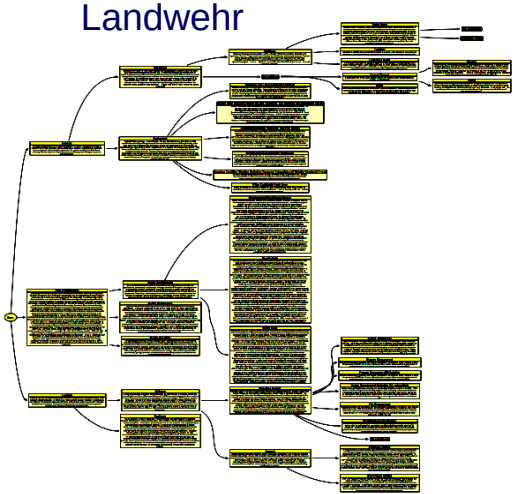


Tool B

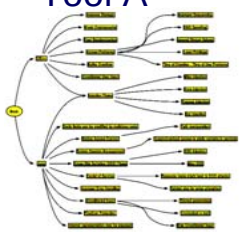
7 Kingdoms



Landwehr



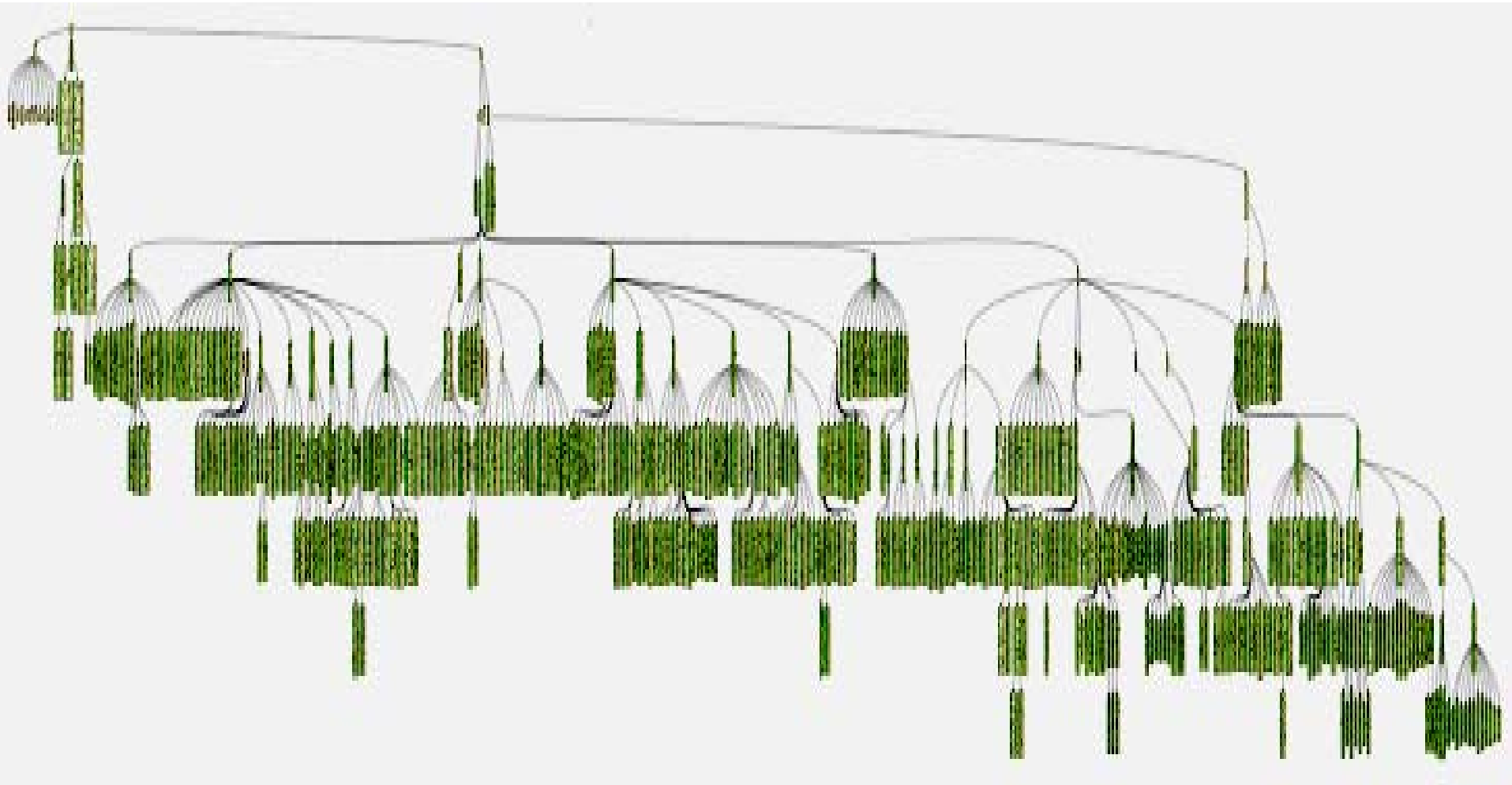
Tool A



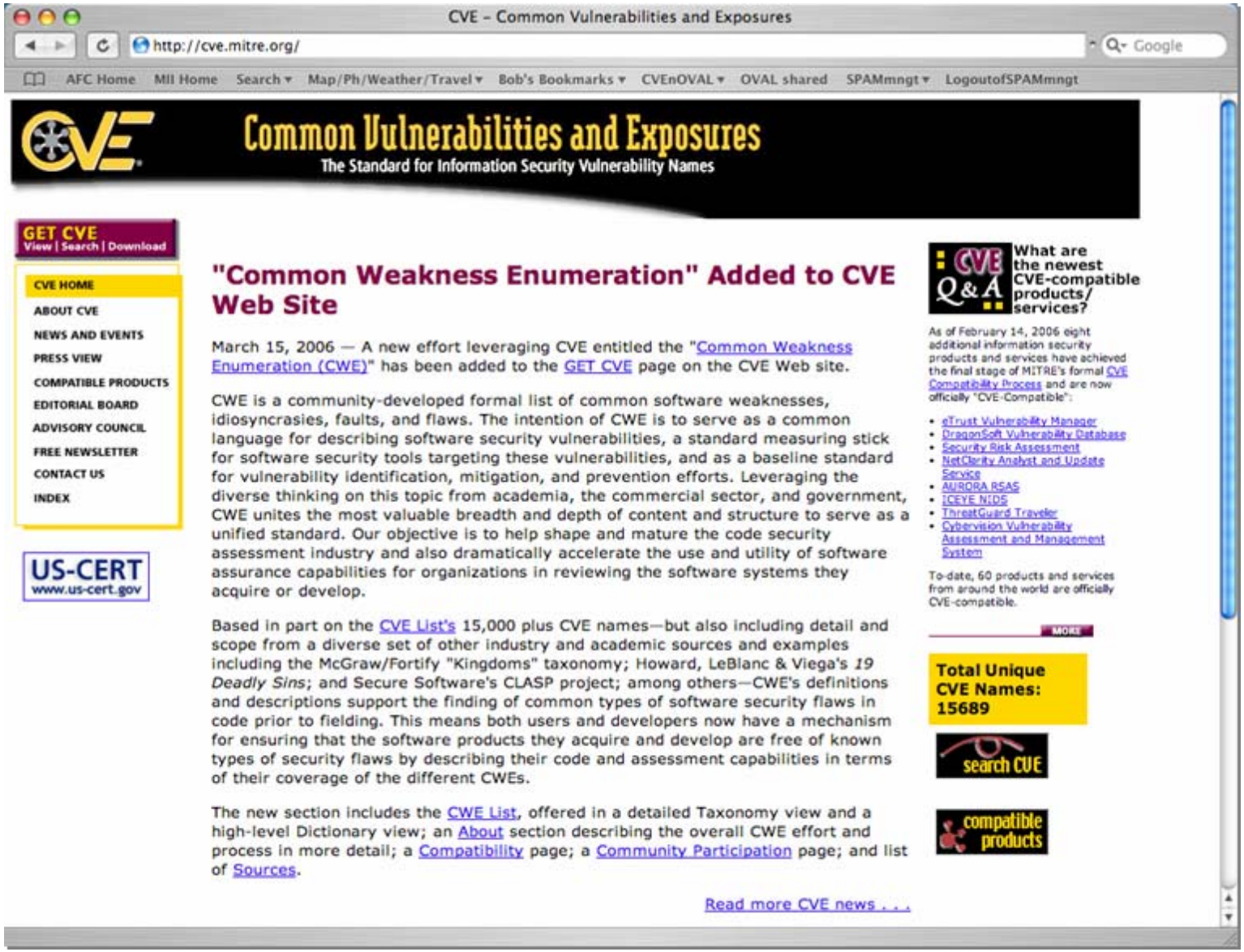
Current Community Contributing to the Common Flaw Enumeration

- Cenzic
- CERT/CC
- Cigital
- CodescanLabs
- Coverity
- DHS
- Fortify
- IBM
- Interoperability Clearing House
- JHU/APL
- Kestrel Technology
- Klocwork
- Microsoft
- MIT Lincoln Labs
- MITRE
- North Carolina State University
- NIST
- NSA
- Oracle
- Ounce Labs
- OWASP
- PARASOFT
- Secure Software
- Security Institute
- Semantic Designs
- SPI Dynamics
- VERACODE
- Watchfire
- WASC
- Whitehat Security, Inc.
- Tim Newsham

Approximately 500 Dictionary Elements



CWE Initial Draft is available



http://cve.mitre.org/cwe/

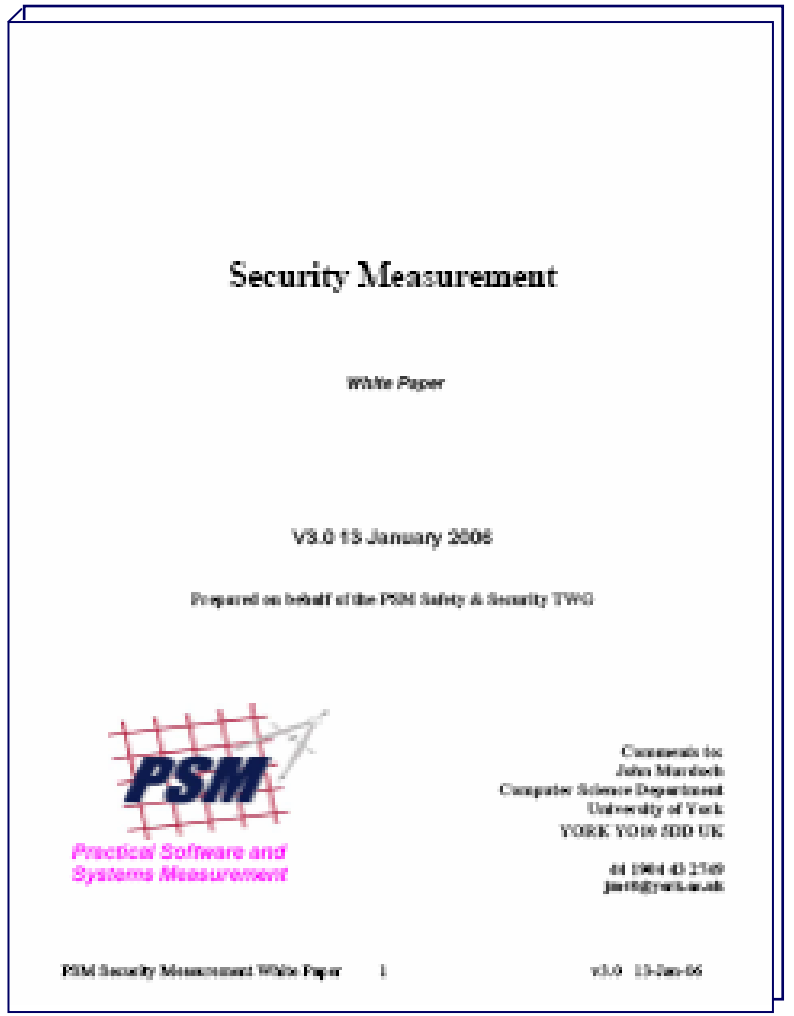
Common Attack Patterns Enumeration and Classification (CAPEC)

- **Service Description**
  - Supports classification taxonomies to be easily understood and consumable by the broad software assurance community and to be aligned and integrated with the other SwA community knowledge catalogs.
- **Service Tasks**
  - Identify and analyze reference Attack Pattern resources from academia, govnt, and industry.
  - Define standard Attack Pattern schema.
  - Identify and collect potential Attack Pattern seedling instances.
  - Finalize scope of effort to clarify number of Attack Patterns to be targeted for initial release.
  - Translate Attack Pattern seedling content into the defined schema.
  - Analyze and extend Attack Pattern seedlings to fulfill schema.
  - Identify set of new Attack Patterns to be authored.
  - Author targeted list of new Attack Patterns.
  - Map all Attack Patterns to the Common WIFF Enumeration and Classification (CWEC).
  - Define a classification taxonomy for Attack Patterns.
  - Map Attack Patterns into the defined classification taxonomy.
  - Publish content to SwA community, solicit input, collaborate, review, and revise as needed.
  - Define process for ongoing extension and sustainment of the CAPEC.
  - Provide assistance to design, build, test, and deploy a website for public hosting of CAPEC.

Homeland Security

Software Security Measurement: Enabling Decision-Making for Measuring Risk Exposure

- Security Measurement: A collaboration among US DHS, US DoD, UK MOD and Australian DMO
- Tasking via Practical Software & Systems Measurement (PSM) Support Center (US Army)
  - PSM Security Measurement draft White Paper
    – Oct 2005
  - Security Measurement Guidance Documentation – May 2006 (PSM Tech WG),
    -- 2 September 2006 (after Users Conf)
  - Measurement Specifications
    -- Sep 2006
  - Security Measurement Training Package
    – Oct 2006
  - Security Measurement Trials Report
    -- September 2007


Security Measurement

White Paper

V3.0 15 January 2006

Prepared on behalf of the PSM Safety & Security TWG

PSM
Practical Software and Systems Measurement

Comments to:
John Murdoch
Computer Science Department
University of York
YORK YO10 5DD UK

PSM Security Measurement White Paper 1 v3.0 13-Jan-06

Homeland Security

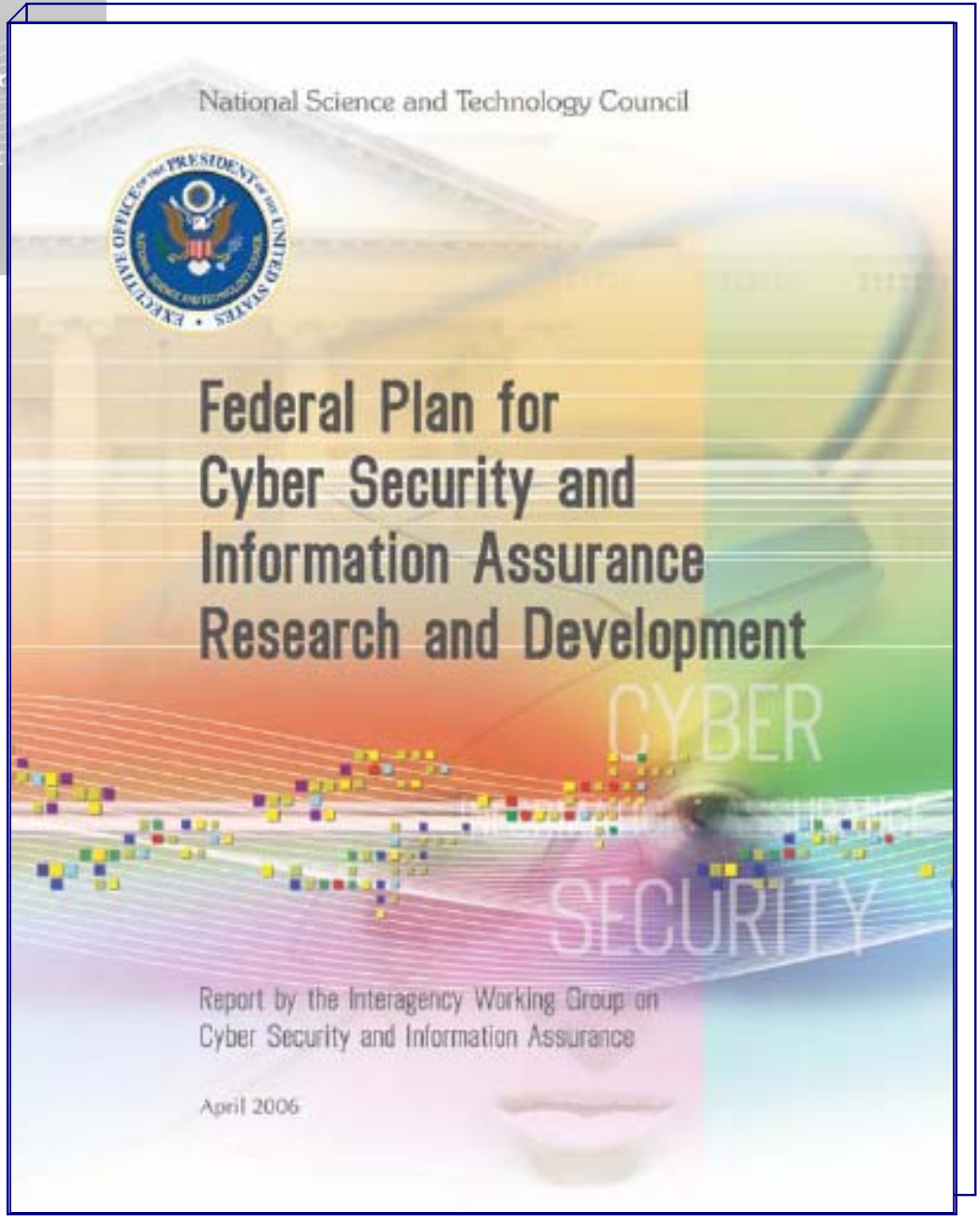
www.psmsc.com

Software Assurance R&D

- Identify SwA R&D; coordinating requirements and priorities with other federal agencies
  - Advocate funding of SwA R&D through the DHS S&T Directorate
    - examine tools and techniques for analyzing software to detect security vulnerabilities and techniques that require access to source code & binary-only techniques;
  - Advocate SwA priorities through multi-agency Technical Support Working Group
    - Identify SwA R&D for combating terrorism (www.tswg.gov)
    - Support TSWG SwA R&D on secure software engineering
  - Update R&D needs & priorities specific for SwA
    - list available via SwA Technology WG on https://us-cert.esportals.net/
  - Contribute to multi-agency Cyber Security and IA R&D provided to stakeholders.

Homeland Security

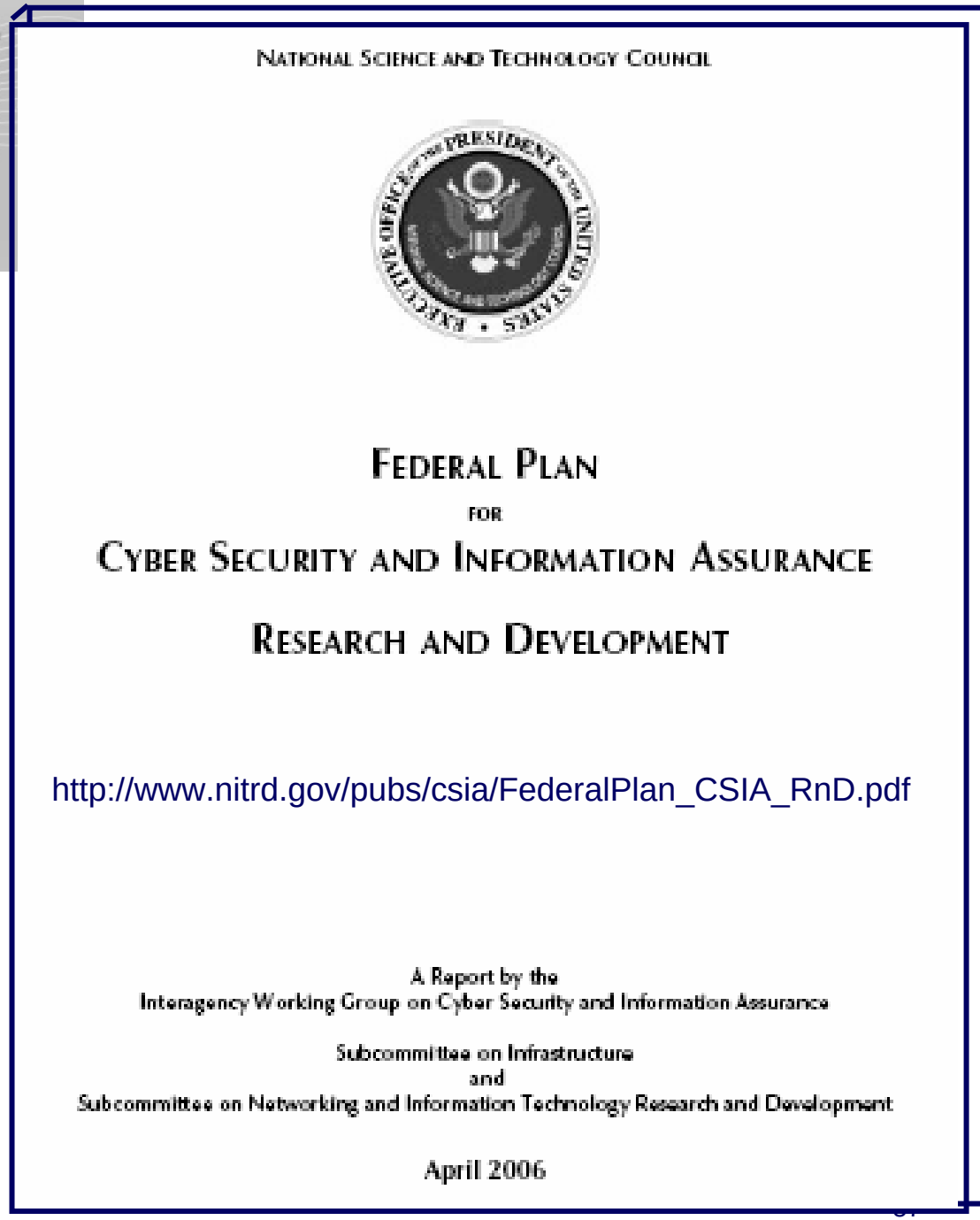
http://www.nitrd.gov



Homeland Security

1. **Functional Cyber Security**
2. **Securing the Infrastructure**
3. **Domain-Specific Security**
4. **Cyber Security Characterization and Assessment**
5. **Foundations for Cyber Security**
6. **Enabling Technologies for Cyber Security & IA**
7. **Advanced & Next Generation Systems & Architecture for Cyber Security**
8. **Social Dimensions of Cyber Security**

Homeland Security



NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

FEDERAL PLAN

FOR

CYBER SECURITY AND INFORMATION ASSURANCE

RESEARCH AND DEVELOPMENT

http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf

A Report by the
Interagency Working Group on Cyber Security and Information Assurance

Subcommittee on Infrastructure
and
Subcommittee on Networking and Information Technology Research and Development

April 2006

1. Functional Cyber Security
2. Securing the Infrastructure
3. Domain-Specific Security
4. Cyber Security Characterization and Assessment
5. Foundations for Cyber Security
6. Enabling Technologies for Cyber Security & IA
7. Advanced & Next Generation Systems & Architecture for Cyber Security
8. Social Dimensions of Cyber Security

Homeland Security

Top Priorities Technical / Funding

Attack protection, prevention, & preemption

Automated attack detection, warning & response

Secure process control systems

Wireless security

Software quality assessment & fault characterization

Software testing & assessment tools

Secure software engineering

Analytical techniques for security across the IT systems engineering life cycle

Cyber Security & IA R&D testbeds

Trusted computing base architectures

Inherently secure, high-assurance, and provably secure systems & architectures

http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf

Bi-Monthly Software Assurance (SwA) Working Groups:

next will be held July 18-20 at Booz Allen Hamilton at 3811 N. Fairfax Drive, Suite 600 Arlington, VA 22203. Please note the Tuesday and Thursday sessions are all-day sessions with a break at 11:30 for lunch.

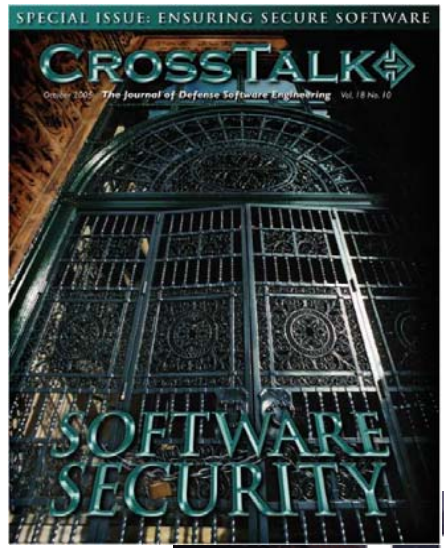
	Tuesday, July 18th	**Wednesday, July 19th**	**Thursday, July 20th**
Morning 9:00am - 11:30am	Session 1: Business Case WG	Plenary Session	Session 5: Acquisition WG
	Session 2: Processes/Practices (standards) WG		Session 6: Measurement WG
Afternoon 1pm - 5pm	Session 1: Business Case WG	Session 3: Technology, Tools & Product Evaluation WG	Session 5: Acquisition WG
	Session 2: Processes/Practices (standards) WG	Session 4: Workforce Education & Training WG	Session 6: Measurement WG

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.

Homeland Security

DHS Software Assurance Outreach Services

- Co-sponsor semi-annual Software Assurance Forum for government, academia, and industry to facilitate the ongoing collaboration -- next October 2006
- Sponsor SwA issues of CROSSTALK (Oct 05 & Sep 06), and provide SwA articles in other journals to "spread the word" to relevant stakeholders
- Provide free SwA resources via "BuildSecurityIn" portal to promote relevant methodologies
- Provide DHS Speakers Bureau speakers
- Support efforts of consortiums and professional societies in promoting SwA



INPUT TargetVIEW

Homeland Security

Software Assurance Observations

- Business/operational needs are shifting to now include “resiliency”
  - Investments in process/product improvement and evaluation must include security
  - Incentives for trustworthy software need to be considered with other business objectives -- measurement needed to better support IT security decision-making
- Pivotal momentum gathering in recognition of (and commitment to) process improvement in acquisition, management and engineering
  - Security requirements need to be addressed along with other functions
  - Software assurance education and training is a key enabler
- From a national/homeland security perspective, acquisition and development “best practices” must contribute to safety and security
  - More focus on “supply chain” management is needed to reduce risks
    - National & international standards need to evolve to “raise the floor” in defining the “minimal level of responsible practice” for software assurance
    - Qualification of software products and suppliers’ capabilities are some of the important risk mitigation activities of acquiring and using organizations
  - In collaboration with industry and academia, Federal agencies need to focus on software assurance as a means of better enabling operational resiliency

Homeland Security

DHS Software Assurance Program

- Program goals promote security for software throughout the lifecycle:
  - Secure and reliable software supporting mission operational resiliency *
  - Better trained and educated software developers using development processes and tools to produce secure software
  - Informed customers demanding secure software, with requisite levels of integrity, through improved acquisition strategies. *
- Program objectives are to:
  - Shift security paradigm from Patch Management to SW Assurance.
  - Encourage the software developers (public and private industry) to raise the bar on software quality and security.
  - Partner with the private sector, academia, and other government agencies in order to improve software development and acquisition processes.
  - Facilitate discussion, develop practical guidance, development of tools, and promote R&D investment.

Homeland Security

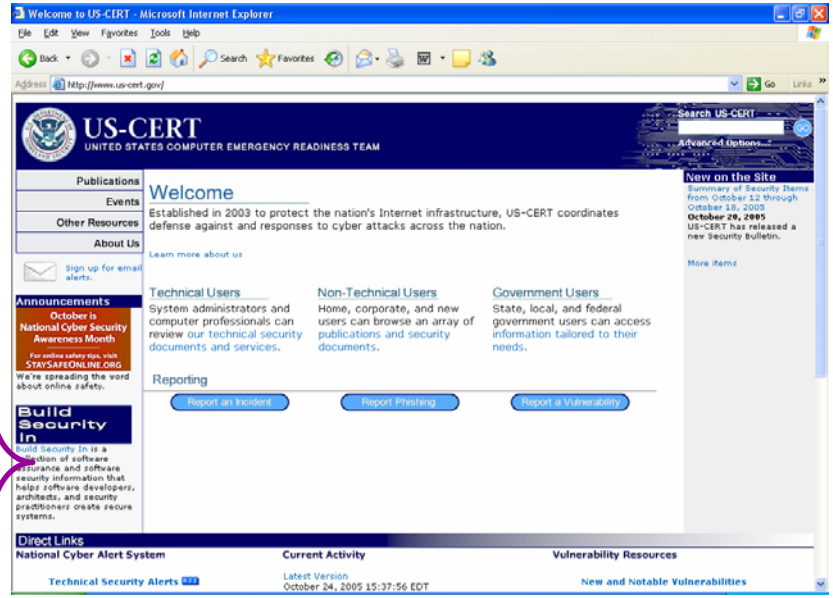
* Guiding principles in the National Strategy to Secure Cyberspace provide focus on “producing more resilient and reliable information infrastructure,” and includes “cyber security considerations in oversight activities.”

Achieving Software Assurance – in the future

- **Consumers will have expectations for product assurance:**
  - Information about evaluated products will be available along with responsive provisions for discovering exploitable vulnerabilities throughout the lifecycle, including risks from reuse of legacy software;
  - Information on suppliers' process capabilities (business practices) will be used to determine security risks posed by the suppliers' products and services to acquisition projects and to the operations enabled by the software.
- **Suppliers will be able to distinguish their companies by delivering quality products with requisite integrity and be able to make assurance claims about the IT/software safety, security and dependability:**
  - Relevant standards will be used from which to base business practices and to make assurance claims;
  - IT/software workforce will have requisite knowledge/skills for developing secure, quality products, and
  - Qualified tools will be used in software lifecycle to enable developers and testers to mitigate risks.

Semi-Annual Software Assurance Forum -- Next in Oct 2006

www.us-cert.gov →



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

SwA Discussion and Q&A at CISSE
(June 7th at 4:15pm in Rm 1109)

- - - - - - - -

Back-up Slides