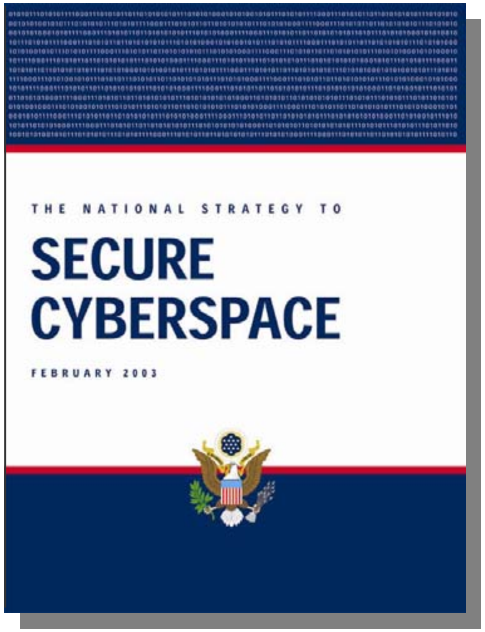
Software Assurance:

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



THE NATIONAL STRATEGY TO

SECURE CYBERSPACE

FEBRUARY 2003

Considerations for Advancing a National Strategy to Secure Cyberspace

Sept 7, 2005

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

Mission to Secure Cyberspace

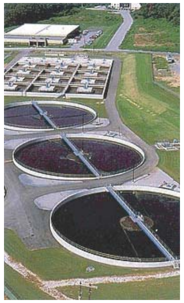
The National Cyber Security Division (NCSD) mission, in cooperation with public, private, and international entities, is to secure cyberspace and America’s cyber assets.

Mission components include:

- Implementation of the *National Strategy to Secure Cyberspace* and Homeland Security Presidential Directive #7 (HSPD#7)
- Implementation of priority protective measures to secure cyberspace and to reduce the cyber vulnerabilities of America’s critical infrastructures

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

Driving Needs for Software Assurance

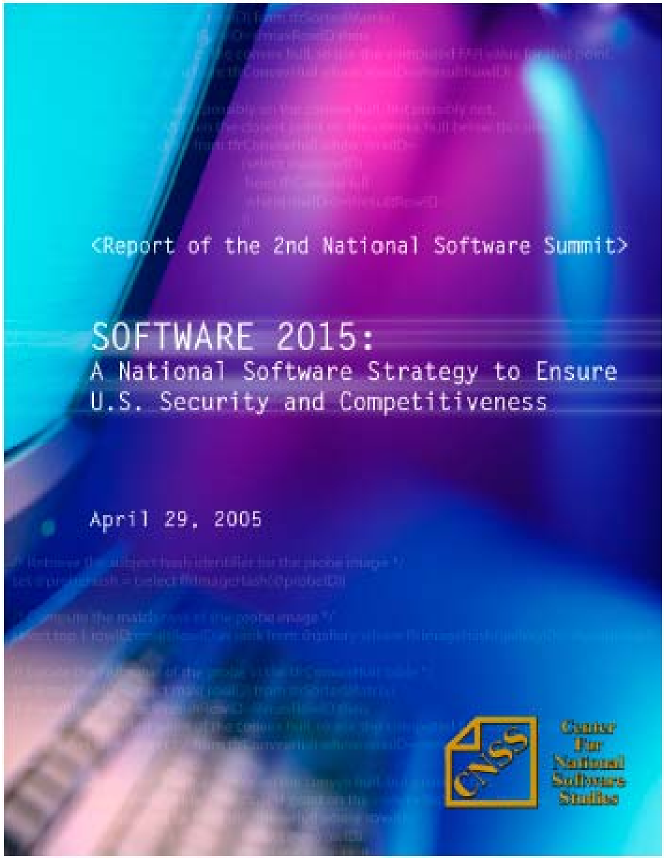
- Software vulnerabilities jeopardize intellectual property, business operations and services, infrastructure operations, and consumer trust
- Growing awareness and concern over the ability of an adversary to subvert the software supply chain
  - Federal Government relies on COTS products and commercial developers using foreign and non-vetted domestic suppliers to meet majority of IT requirements
  - Software development offers opportunities to insert malicious code and to poorly design and build software enabling exploitation
- Growing concern about inadequacies of suppliers’ capabilities to build and deliver secure software with requisite levels of integrity
  - Current education & training provides too few practitioners with requisite competencies in secure software engineering
  - Concern about suppliers not exercising “minimum level of responsible practice”
  - Growing need to improve both the state-of-the-practice and the state-of-the-art on software capabilities of the nation
- Processes and technologies are required to build trust into software acquired and used by Government and critical infrastructure

Strengthen operational resiliency

United States 2nd National Software Summit

Report April 29, 2005*

- Identified major gaps in:
  - Requirements for software tools and technologies to routinely develop error-free software and the state-of-the-art
  - State-of-the-art and state-of-the-practice
- Recommended elevating software to national policy
  - through implementation of “Software 2015: a National Software Strategy to Ensure US Security and Competitiveness”
  - to be pursued through public-private partnerships involving government, industry and academia



<Report of the 2nd National Software Summit>

SOFTWARE 2015:
A National Software Strategy to Ensure
U.S. Security and Competitiveness

April 29, 2005

CNSS Center For National Software Studies

- Purpose of National Software Strategy:
  - Achieve ability to routinely develop and deploy trustworthy software products
  - Ensure the continued competitiveness of the US software industry

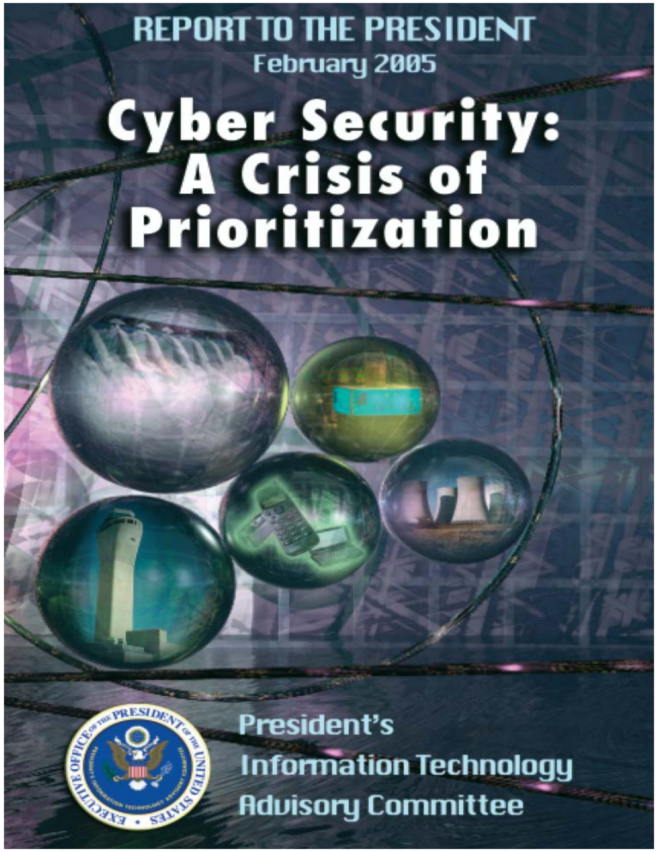
*** See report at Center for National Software Studies   www.cnsoftware.org/nss2report**

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.



REPORT TO THE PRESIDENT
February 2005

Cyber Security:
A Crisis of
Prioritization

President's
Information Technology
Advisory Committee

* 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'

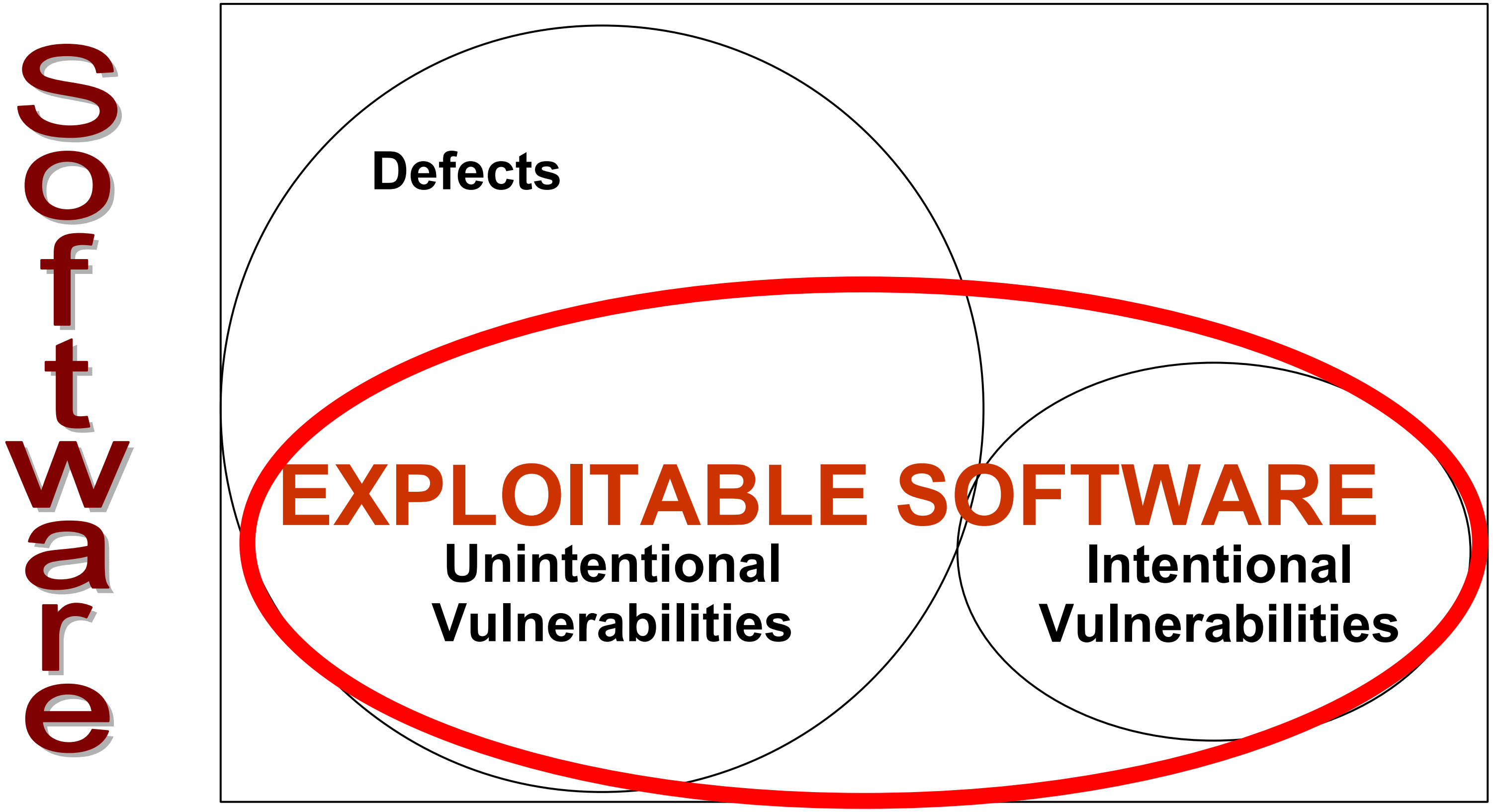
GAO Reports relative to Software Assurance

- GAO-04-321 Report, **“Cybersecurity for Critical Infrastructure Protection,”** May 2004
- GAO-04-678 Report, **“Defense Acquisitions: Knowledge of Software Suppliers Needed to Manage Risks,”** May 2004
  - Outsourcing, foreign development risks & insertion of malicious code
  - DoD noted domestic development subject to similar risks
  - Recommendations for program managers to factor in software risks and security in risk assessments
- GAO-05-434 Report, **“Critical Infrastructure Protection: DHS Faces Challenges in Fulfilling Cybersecurity Responsibilities,”** May 2005
- Current GAO study on “risks attributable to outsourcing of software throughout critical infrastructure,” to be published Nov 2005

Exploitable Software:

Outcomes of non-secure practices and/or malicious intent

Exploitation potential of vulnerability independent of "intent"



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

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

Why Software Assurance is Critical

- 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 unvetted software supply chain (COTS & custom)
  - Attack sophistication (easing exploitation)
  - Reuse (unintended consequences increasing number of vulnerable targets)
  - Number of vulnerabilities and incidents
  - Number of 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

What has Caused Software Assurance Problem

Increasing software vulnerabilities and exploitation

- Then
  - Domestic dominated market
  - Stand alone systems
  - Software small and simple
  - Software small part of functionality
  - Custom and closed development processes (cleared personnel)
  - Adversaries known, few, and technologically less sophisticated

- Now
  - Global market
  - Globally network environment
  - Software large and complex
  - Software is the core of system functionality
  - COTS/GOTS/Custom in open and unknown, un-vetted development processes with outsourcing & reuse (foreign sourced, un-cleared, un-vetted)
  - Adversaries numerous and sophisticated

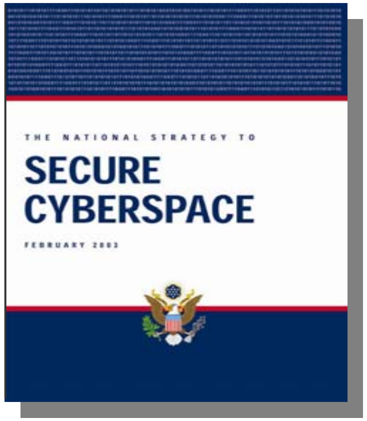
Exploitation of Software Vulnerabilities

- Serve as primary points of entry that attackers may attempt to use to gain access to systems and/or data
- Enable compromise of business and missions
- Allow Attackers to:
  - Pose as other entities
  - Execute commands as other users
  - Conduct information gathering activities
  - Access data (contrary to specified access restrictions for that data)
  - Hide activities
  - Conduct a denial of service
  - Embed malicious logic for future exploitation

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.”



THE NATIONAL STRATEGY TO
SECURE
CYBERSPACE
FEBRUARY 2003

- DHS Program goals promote the security of software across the development 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

Software Assurance Program Alignment

THE NATIONAL STRATEGY TO SECURE CYBERSPACE FEBRUARY 2003	*National Strategy to Secure Cyberspace*					*HSPD-7*
	Priority 1: National Cyberspace Security Response System	**Priority 2:** National Cyberspace Threat and Vulnerability Reduction Prog.	**Priority 3:** National Cyberspace Security Awareness and Training Prog.	**Priority 4:** Securing Govt.'s Cyberspace	**Priority 5:** International Cyberspace Security Cooperation	"…maintain an organization to serve as a focal point for the security of cyberspace.."
NCSD Goal 1: Prevent, detect, and respond to cyber incidents, and reconstitute rapidly after cyber incidents.	✓			✓	✓	✓
NCSD Goal 2: Work with public and private sectors to reduce vulnerabilities and minimize the severity of cyber attacks.		✓	✓	✓	✓	✓
NCSD Goal 3: Promote a comprehensive national awareness program to empower all Americans to secure their own parts of cyberspace.		✓	✓			✓
NCSD Goal 4: Foster adequate training and education programs to support the Nation's cyber security needs.	✓	✓		✓		✓
NCSD Goal 5: Coordinate with the intelligence and law enforcement communities to identify and reduce threats to cyber space.	✓	✓	✓	✓	✓	✓

Software Assurance Program alignment

*"National Strategy to Secure Cyberspace" and Homeland Security Presidential Directive #7

Software Assurance Program Alignment

	National Strategy to Secure Cyberspace					*HSPD7*
	Priority 1: National Cyberspace Security Response System	**Priority 2: National Cyberspace Threat and Vulnerability Reduction Program**	**Priority 3: National Cyberspace Security Awareness and Training Program**	**Priority 4: Securing Govt.'s Cyberspace**	**Priority 5: International Cyberspace Security Cooperation**	**HSDP7: "…maintain an organization to serve as a focal point for the security of cyberspace.."**
NCSD Goal 2: Work with public and private sectors to reduce vulnerabilities and minimize the severity of cyber attacks.		SW Security in the SDLC Developers Guide Build Security In Web site	SwA Common Body of Knowledge	Tools and Product Evaluation NIST Metrics and Tool Evaluation NIAP Review	Processes and Practices NIST/IEEE ISO/IEC	Software Assurance Program Management

Software Assurance Program Overview

- 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.

* 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."

Software Assurance Program Structure

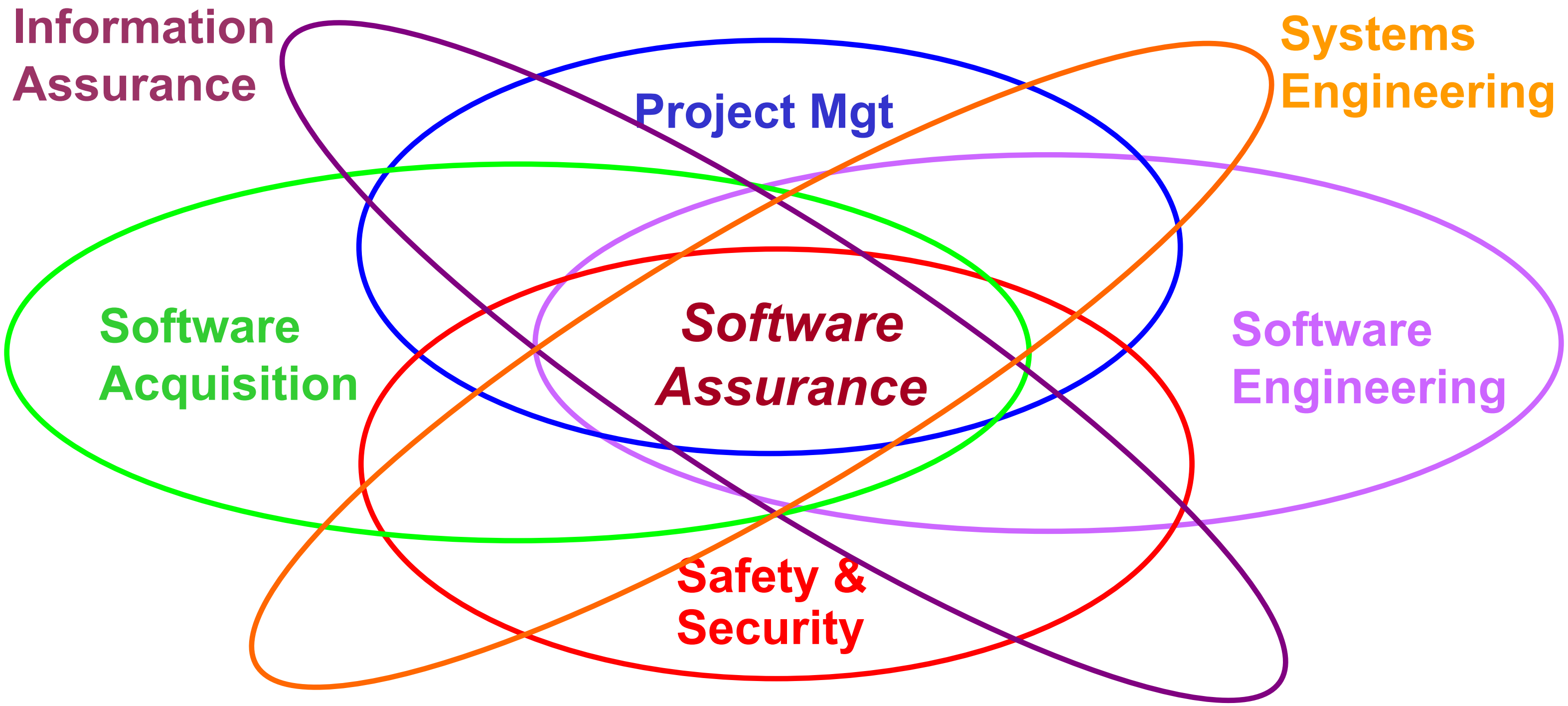
- Program framework encourages the production and acquisition of better quality and more secure software and leverages resources to target the following four areas:
  - People – developers (includes education and training) and users
  - Processes – best practices, standards, and practical guidelines for the development of secure software
  - Technology – evaluation tools and cyber security R&D
  - Acquisition – software security improvements through specifications and guidelines for acquisition and outsourcing

Software Assurance: People

- Provide Software Assurance Common Body of Knowledge (CBK) framework to identify workforce needs for competencies, leverage "best practices" and guide curriculum development for Software Assurance education and training**
  - Hosted Electronic Develop a Curriculum Event and CBK Working Groups (April, June and August 2005) to develop CBK that involved participation from academia, industry and Federal Government
  - Addressing three domains: "acquisition & supply," "development," and "post-release assurance" (sustainment)
  - Distribute CBK v0.6 in October 2005, with v.0.8 in Jan 2006 and v1.0 by March 2006
  - Develop CBK awareness materials, including Frequently Asked Questions by Oct 2005 with update in January, 2006
  - Develop a pilot training/education curriculum consistent with CBK in conjunction with early adopters for distribution by September 2007

**NCSD Goal Action 2.3.1

Disciplines Contributing to SwA CBK



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

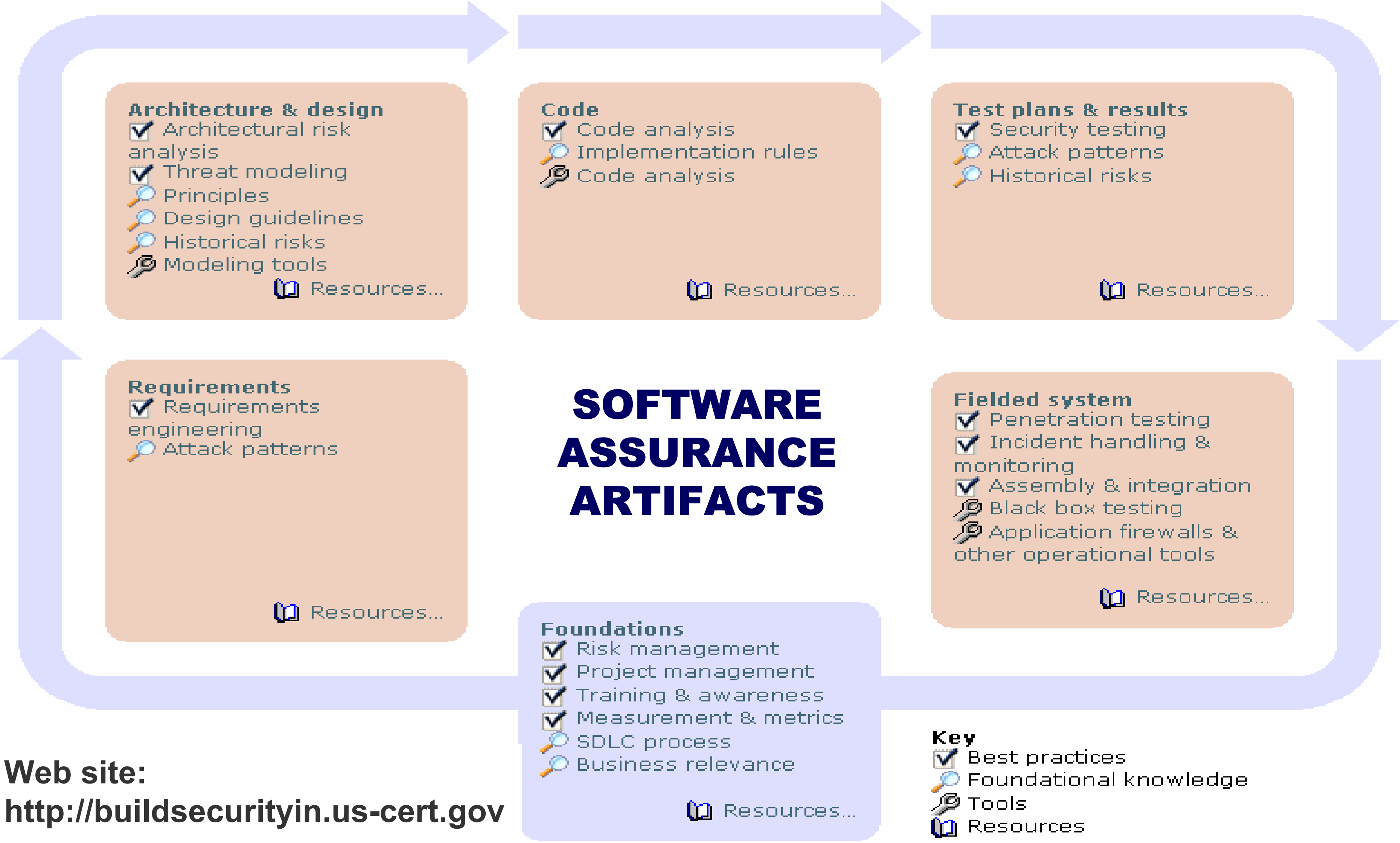
- A “knowledge area” extension within each of the contributing disciplines;
- A stand-alone CBK drawing upon contributing disciplines;
- A set of functional roles, drawing upon a common body of knowledge; allowing more in-depth coverage dependent upon the specific roles.

Software Assurance: Process

- Provide practical guidance in software assurance process improvement methodologies**
  - Co-sponsor semi-annual Software Assurance Forum for government, academia, and industry to facilitate the ongoing collaboration held April 2005, **3-4 October 2005 at Hilton McLean** and 16-17 March 2006
    - https://www.seeuthere.com/event/m2c757235982986148
  - Collect, develop, and publish practical guidance and reference materials for Security through the Software Development Life Cycle for training software developers in software assurance process improvement methodologies.
    - "SECURING THE SOFTWARE LIFECYCLE: Making Application Development Processes – and Software Produced by Them – More Secure"
  - Sponsoring work with *Software Engineering Institute* and industry to develop a web-based central repository "Build Security In" on US-CERT web site "**buildsecurityin.us-cert.gov** for dissemination of recommended standards, practices, and technologies for secure software development to launch October 2005

**NCSD Goal Action 2.3.2

SwA Process: Lifecycle Touch Points



Architecture & design
- ✓ Architectural risk analysis
- ✓ Threat modeling
- 🔍 Principles
- 🔍 Design guidelines
- 🔍 Historical risks
- 🔧 Modeling tools

📖 Resources...

Code
- ✓ Code analysis
- 🔍 Implementation rules
- 🔧 Code analysis

📖 Resources...

Test plans & results
- ✓ Security testing
- 🔍 Attack patterns
- 🔍 Historical risks

📖 Resources...

Requirements
- ✓ Requirements engineering
- 🔍 Attack patterns

📖 Resources...

SOFTWARE ASSURANCE ARTIFACTS

Fielded system
- ✓ Penetration testing
- ✓ Incident handling & monitoring
- ✓ Assembly & integration
- 🔧 Black box testing
- 🔧 Application firewalls & other operational tools

📖 Resources...

Foundations
- ✓ Risk management
- ✓ Project management
- ✓ Training & awareness
- ✓ Measurement & metrics
- 🔍 SDLC process
- 🔍 Business relevance

📖 Resources...

Key
- ✓ Best practices
- 🔍 Foundational knowledge
- 🔧 Tools
- 📖 Resources

Web site:
http://buildsecurityin.us-cert.gov

Software Assurance: Process (cont')

- Provide practical guidance in software assurance process improvement methodologies**
  - Develop a business case analysis to support lifecycle use of security best practices
  - Complete the DHS/DoD co-sponsored comprehensive review of the NIAP (National Information Assurance Partnership) to be published Sep 2005
  - Participate in relevant standards bodies; identify software assurance gaps in applicable standards from IEEE, ISO/IEC, NIST, OMG, CNSS, and Open Group and support effort through sponsored Processes and Practices Working group (April, June, August, October, and December 2005 and March, June and September 2006)

**NCSD Goal Action 2.3.2

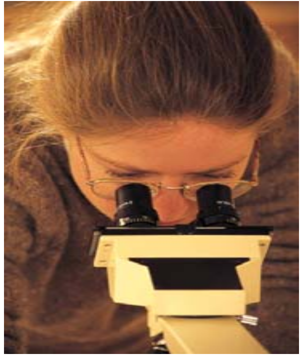
Software Assurance Comes From:

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



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

Reaching the Stakeholders

Leverage Efforts in Evolving ISO Standards, CNSS IA and IEEE CS SWEBOK

Education

- Curriculum
- Accreditation Criteria

CNSS IA Courseware Evaluation

IEEE/ACM Software Engineering 2004 curriculum

University acceptance

Professional Development

- Continuing Education
- Certification

CSDP Online Prep Course

IEEE CS SWE Book Series

Certified Software Development Professional

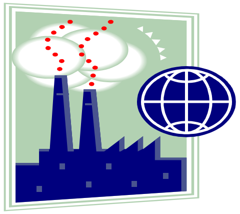
Individual acceptance

Training and Practices

- Standards of Practice
- Training programs

IEEE Software and Systems Engineering Standards Committee

ISO/IEC JTC1/SC7 & SC27 and other committees



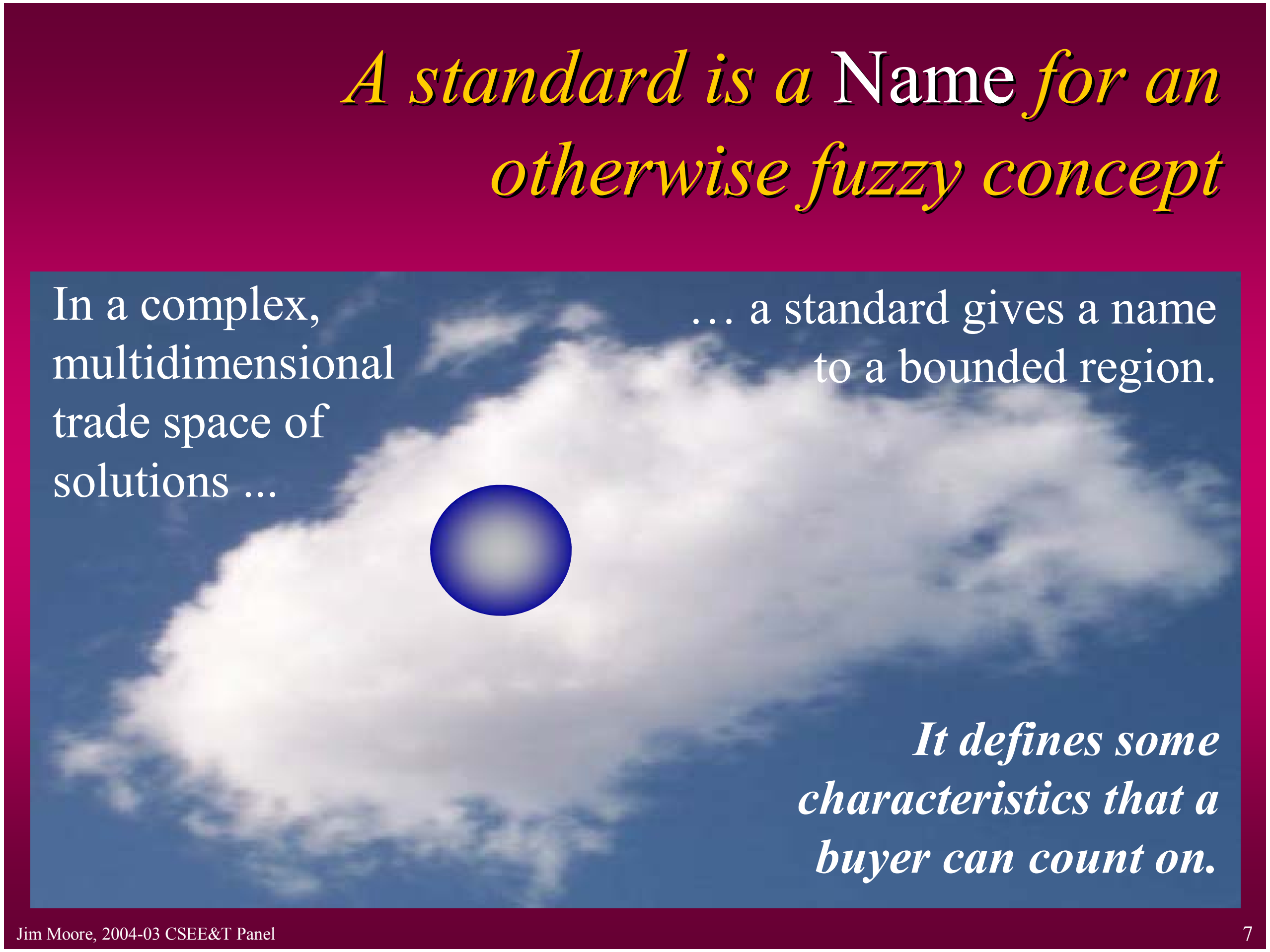
Industrial acceptance

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

Software Assurance Lifecycle Considerations

- Define Lifecycle Threats/Hazards, Vulnerabilities & Risks
- Identify Risks attributable to software
- Determine Threats (and Hazards)
- Understand key aspects of Vulnerabilities
- Consider Implications in Lifecycle Phases:
  - Threats to: System, Production process, Using system
  - Vulnerabilities attributable to: Ineptness (undisciplined practices), Malicious intent, Incorrect or incomplete artifacts, Inflexibility
  - Risks in Current Efforts: Polices & Practices, Constraints

Value of Standards



A standard is a Name *for an otherwise fuzzy concept*

In a complex, multidimensional trade space of solutions ...

… a standard gives a name to a bounded region.

It defines some characteristics that a buyer can count on.

Jim Moore, 2004-03 CSEE&T Panel

7

- ***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,” not necessarily the best available methods

Homeland Security

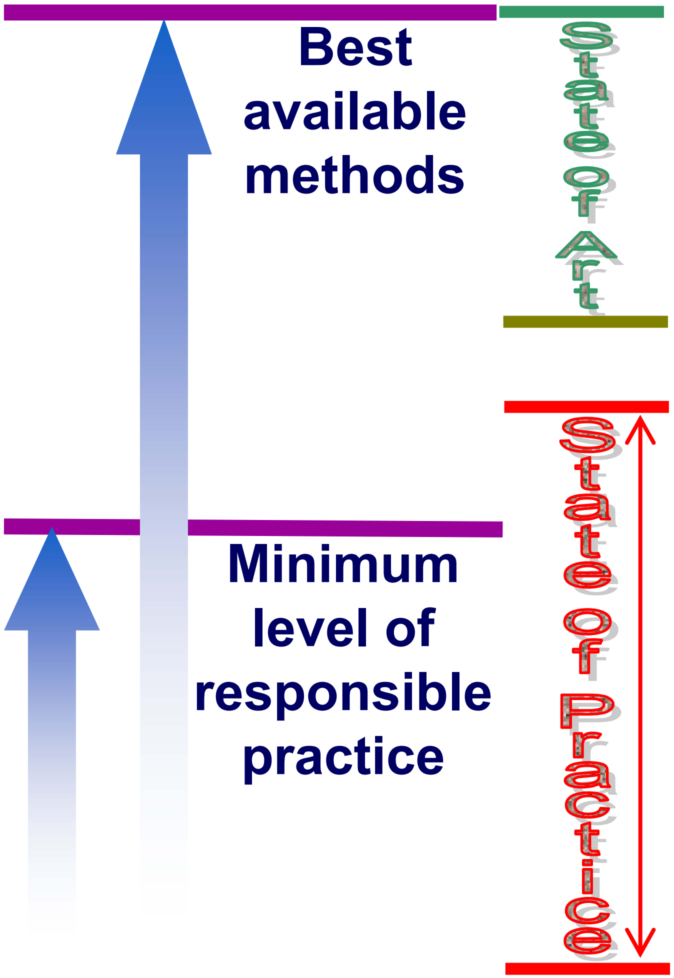
Using Standards and Best Practices to Close gaps between state-of-the-practice and state-of-the-art *[1, 2]

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

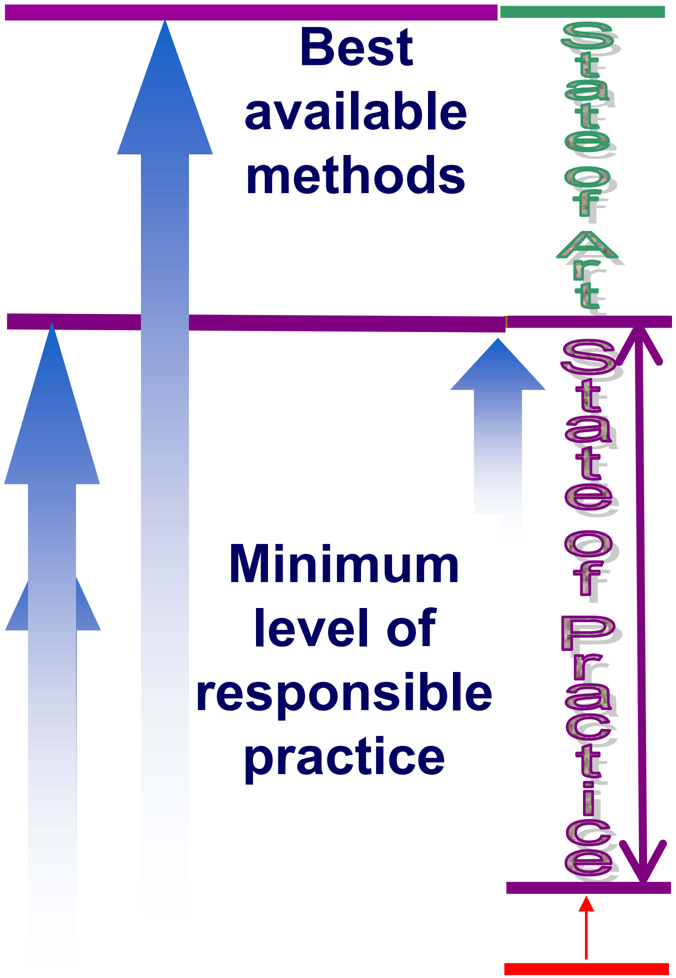
Using Standards and Best Practices to Close gaps between state-of-the-practice and state-of-the-art *1, 2

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.

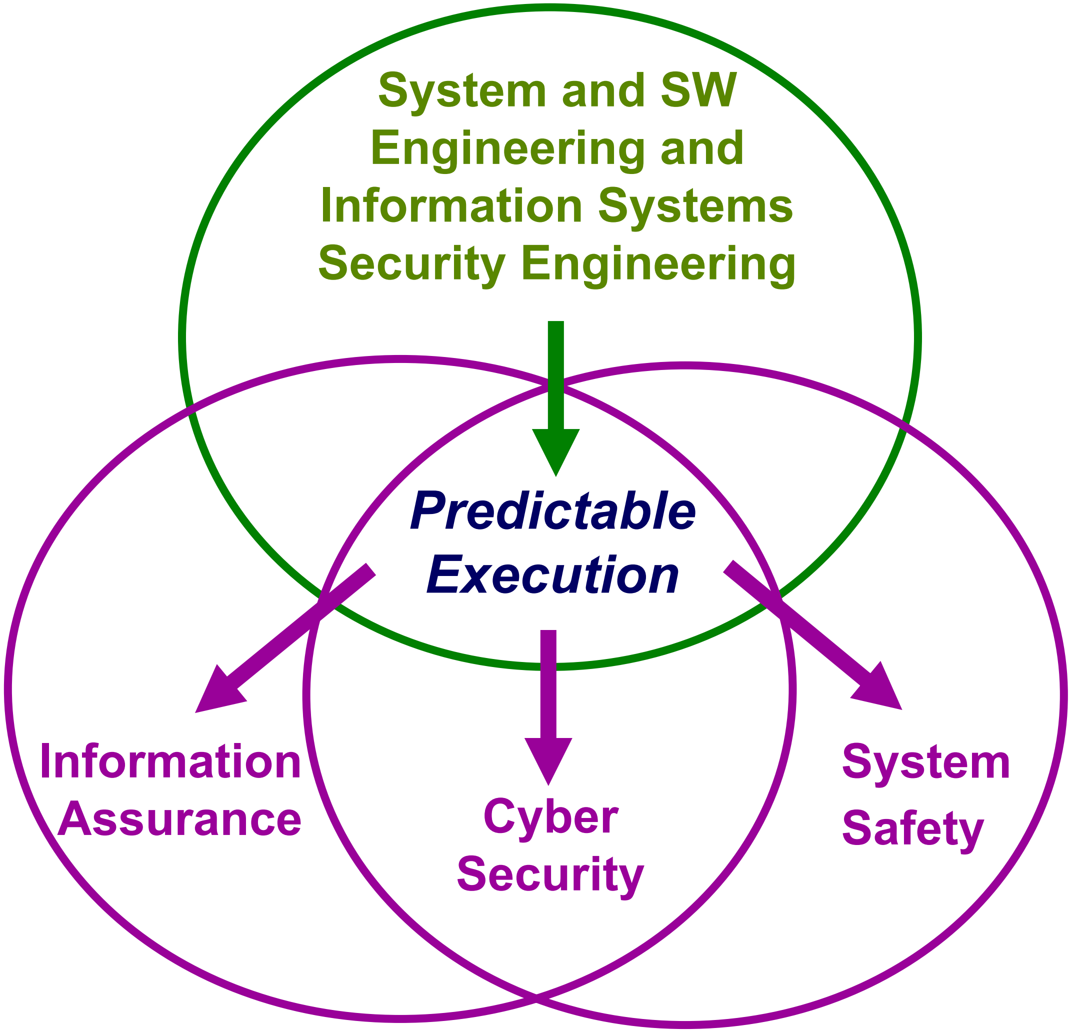
Raising the Floor

- 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


System and SW Engineering and Information Systems Security Engineering
Predictable Execution
Information Assurance
Cyber Security
System Safety

For a safety/security analysis to be valid …

The execution of the system must be *predictable*.

This requires …

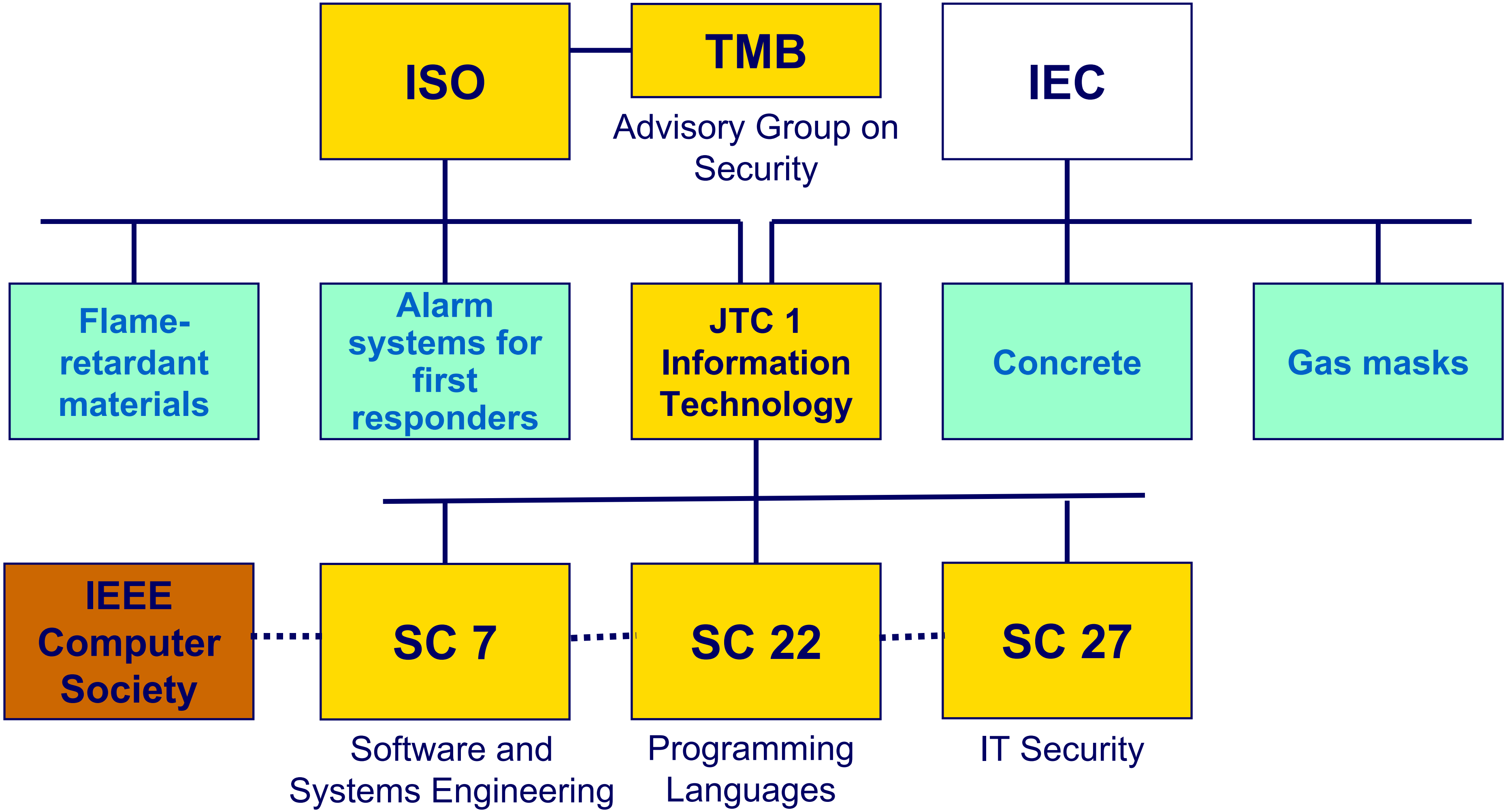
- Correct implementation of requirements, expectations and regulations.
- Exclusion of unwanted function even in the face of attempted exploitation.

Traditional concern

Growing concern

Homeland Security

Security and Assurance Concerns in ISO

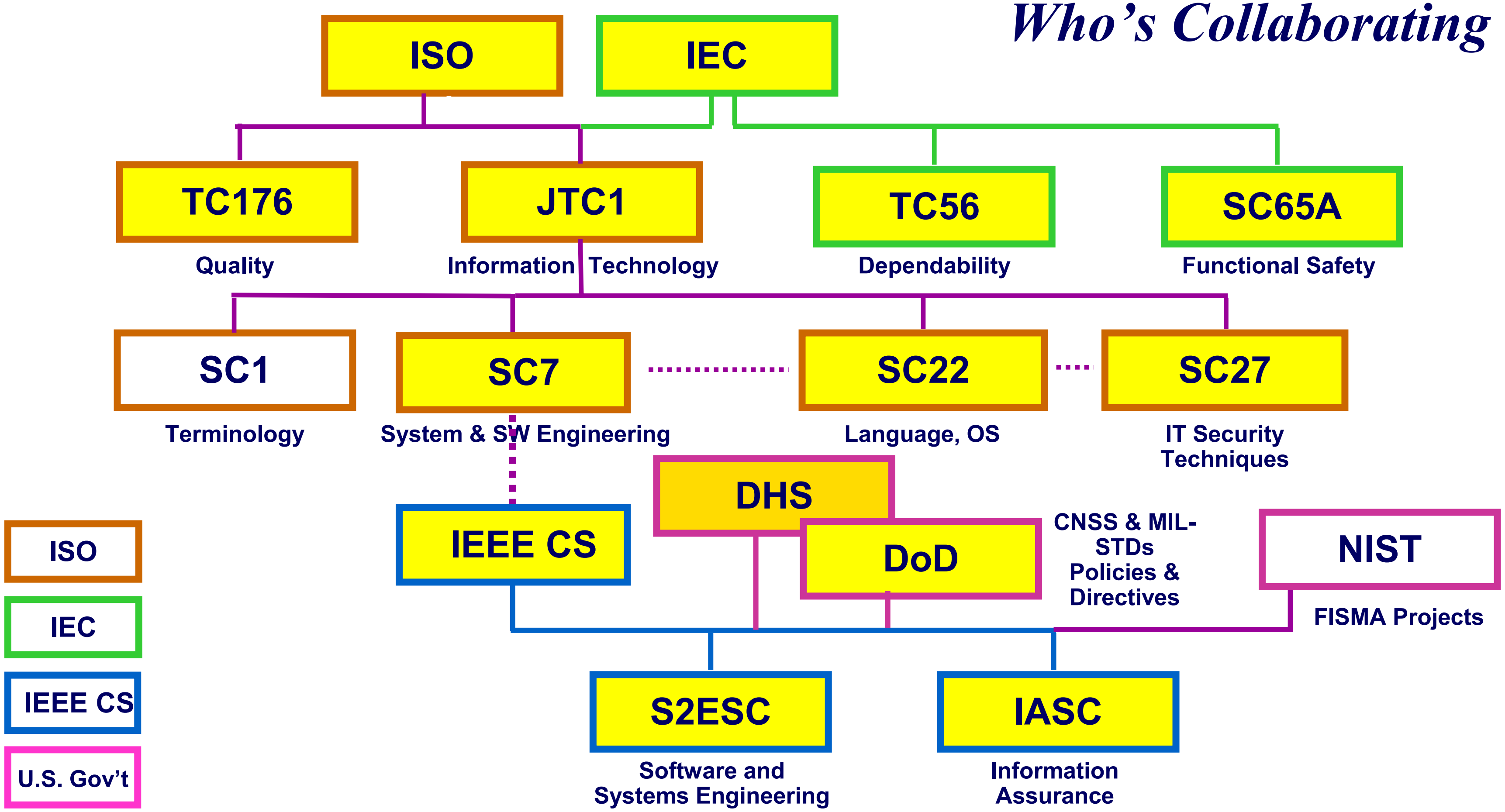

ISO
TMB
Advisory Group on Security
IEC
Flame-retardant materials
Alarm systems for first responders
JTC 1 Information Technology
Concrete
Gas masks
IEEE Computer Society
SC 7
SC 22
SC 27
Software and Systems Engineering
Programming Languages
IT Security

Homeland Security

...... Liaison role between IEEE CS S2ESC and between ISO SCs

Harmonization Efforts Impacting Systems and Software Assurance

Who's Collaborating



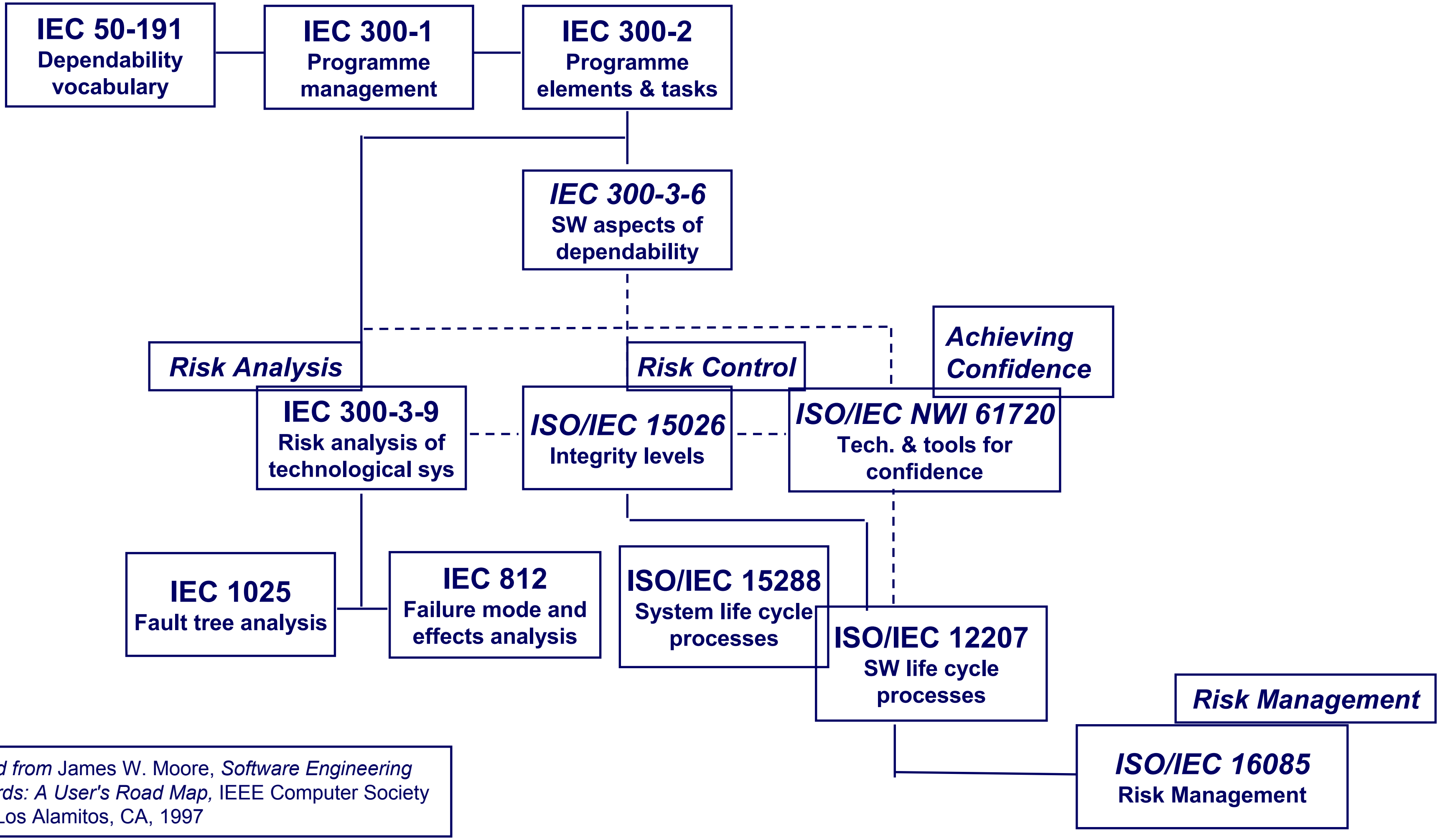
New Scope of ISO 15026 “System and Software Assurance”

“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”

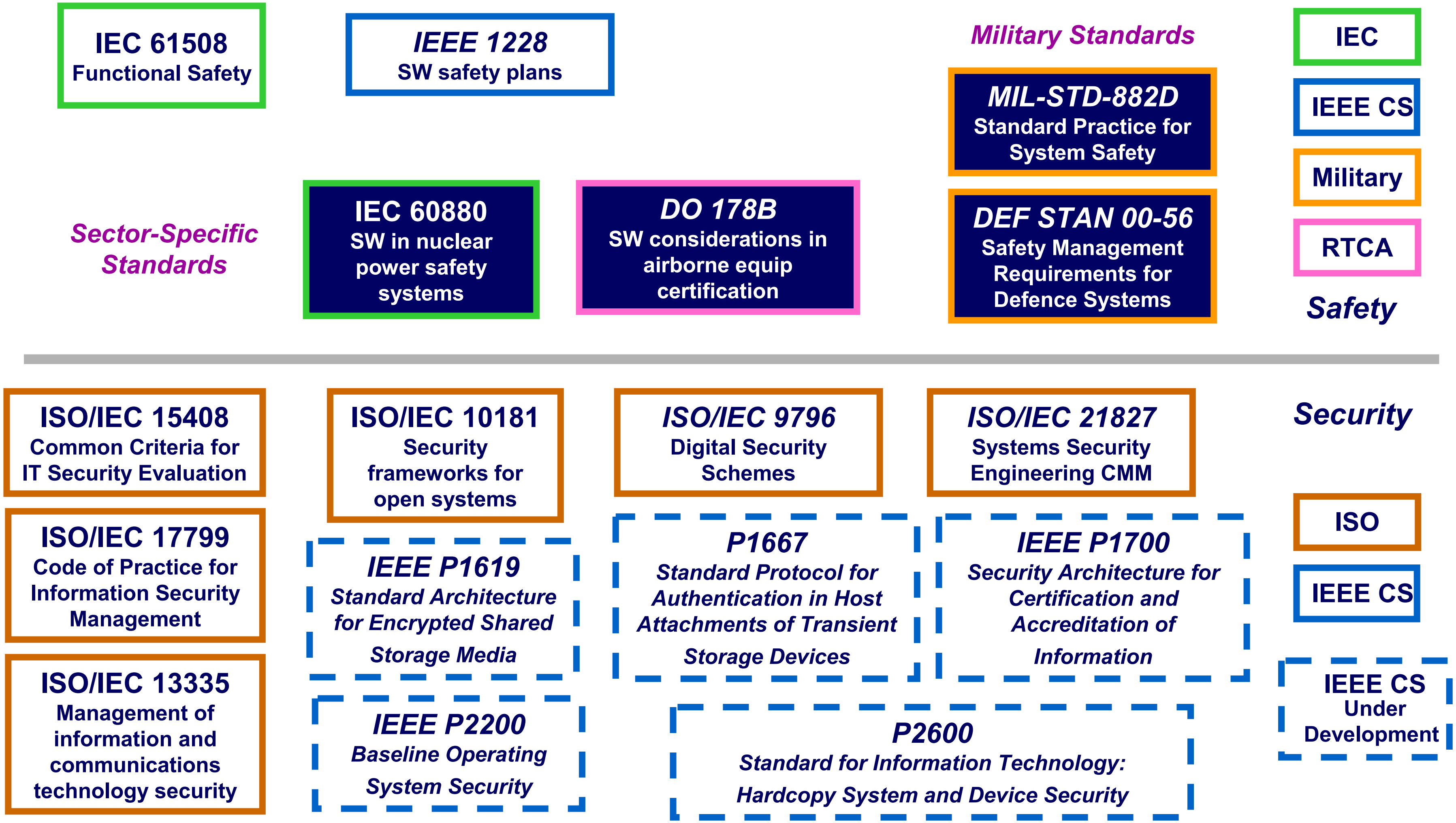
Adopted from Paul Croll’s SSTC 2005 presentation, “Best Practices for Delivering Safe, Secure, and Dependable Mission Capabilities”

Dependability Standards



Adapted from James W. Moore, *Software Engineering Standards: A User's Road Map,* IEEE Computer Society Press, Los Alamitos, CA, 1997

Safety and Security Standards



IEC 61508
Functional Safety

IEEE 1228
SW safety plans

Military Standards

MIL-STD-882D
Standard Practice for System Safety

Sector-Specific Standards

IEC 60880
SW in nuclear power safety systems

DO 178B
SW considerations in airborne equip certification

DEF STAN 00-56
Safety Management Requirements for Defence Systems

IEC

IEEE CS

Military

RTCA

Safety

Security

ISO/IEC 15408
Common Criteria for IT Security Evaluation

ISO/IEC 10181
Security frameworks for open systems

ISO/IEC 9796
Digital Security Schemes

ISO/IEC 21827
Systems Security Engineering CMM

ISO/IEC 17799
Code of Practice for Information Security Management

IEEE P1619
Standard Architecture for Encrypted Shared Storage Media

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

IEEE P1700
Security Architecture for Certification and Accreditation of Information

ISO

IEEE CS

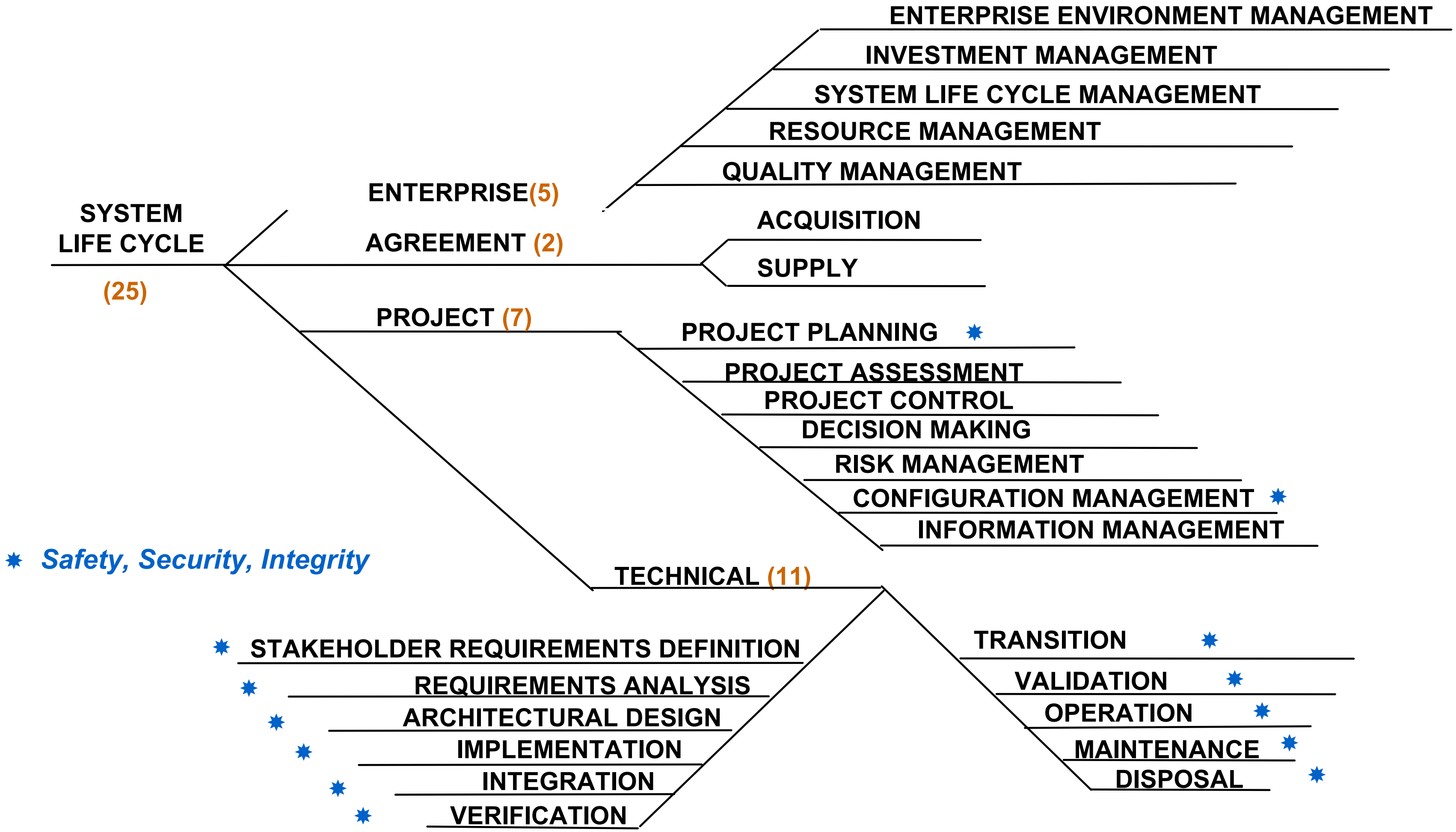
ISO/IEC 13335
Management of information and communications technology security

IEEE P2200
Baseline Operating System Security

P2600
Standard for Information Technology: Hardcopy System and Device Security

IEEE CS
Under Development

Assurance in the ISO/IEC 15288 System Life Cycle Process Framework



SYSTEM LIFE CYCLE (25)

ENTERPRISE (5)
- ENTERPRISE ENVIRONMENT MANAGEMENT
- INVESTMENT MANAGEMENT
- SYSTEM LIFE CYCLE MANAGEMENT
- RESOURCE MANAGEMENT
- QUALITY MANAGEMENT

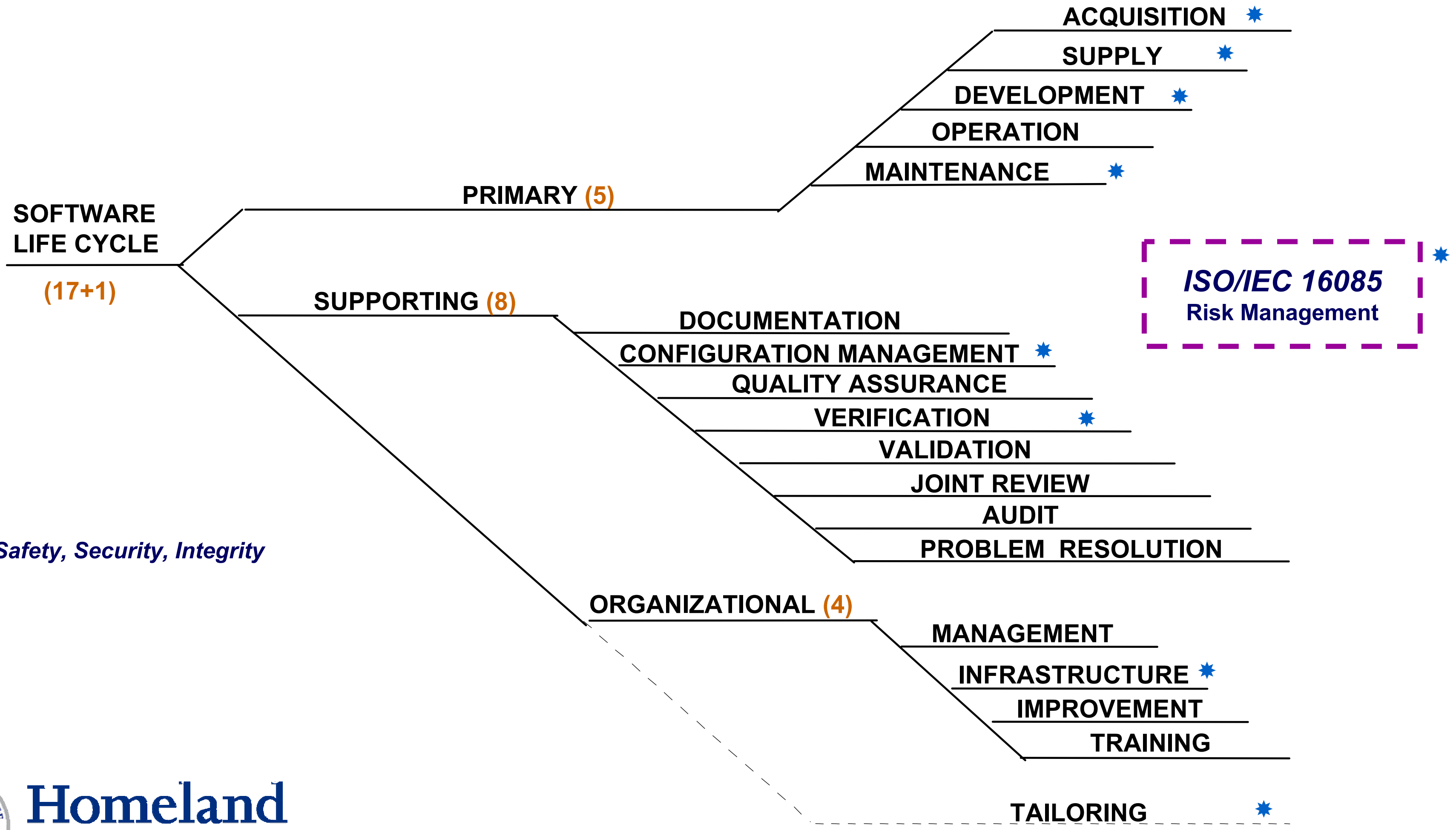
AGREEMENT (2)
- ACQUISITION
- SUPPLY

PROJECT (7)
- PROJECT PLANNING ✸
- PROJECT ASSESSMENT
- PROJECT CONTROL
- DECISION MAKING
- RISK MANAGEMENT
- CONFIGURATION MANAGEMENT ✸
- INFORMATION MANAGEMENT

TECHNICAL (11)
- ✸ STAKEHOLDER REQUIREMENTS DEFINITION
- ✸ REQUIREMENTS ANALYSIS
- ✸ ARCHITECTURAL DESIGN
- ✸ IMPLEMENTATION
- ✸ INTEGRATION
- ✸ VERIFICATION
- TRANSITION ✸
- VALIDATION ✸
- OPERATION ✸
- MAINTENANCE ✸
- DISPOSAL ✸

✸ *Safety, Security, Integrity*

Assurance in the IEEE/EIA 12207 Software Life Cycle Process Framework



SOFTWARE LIFE CYCLE (17+1)

PRIMARY (5)
- ACQUISITION ✸
- SUPPLY ✸
- DEVELOPMENT ✸
- OPERATION
- MAINTENANCE ✸

SUPPORTING (8)
- DOCUMENTATION
- CONFIGURATION MANAGEMENT ✸
- QUALITY ASSURANCE
- VERIFICATION ✸
- VALIDATION
- JOINT REVIEW
- AUDIT
- PROBLEM RESOLUTION

ORGANIZATIONAL (4)
- MANAGEMENT
- INFRASTRUCTURE ✸
- IMPROVEMENT
- TRAINING

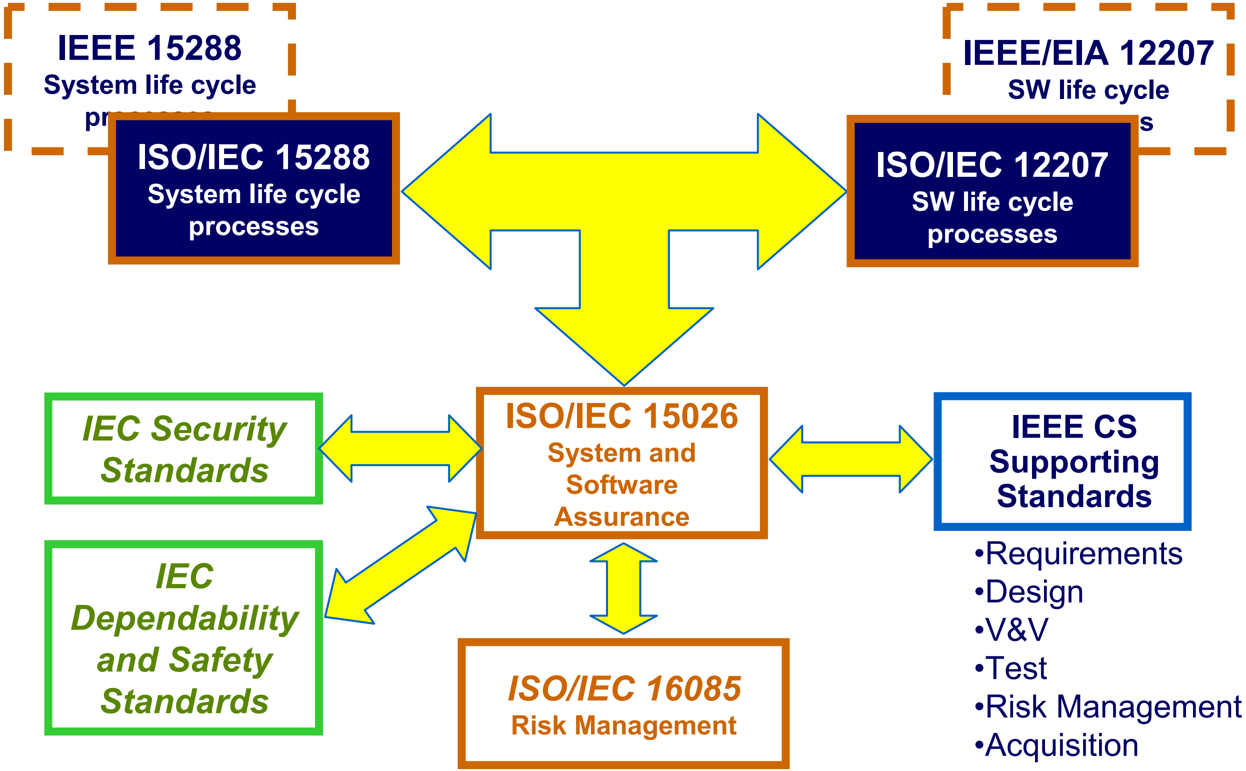
TAILORING ✸

ISO/IEC 16085 Risk Management ✸

✸ *Safety, Security, Integrity*

Harmonization Efforts Impacting Systems and Software Assurance

What's Being Harmonized



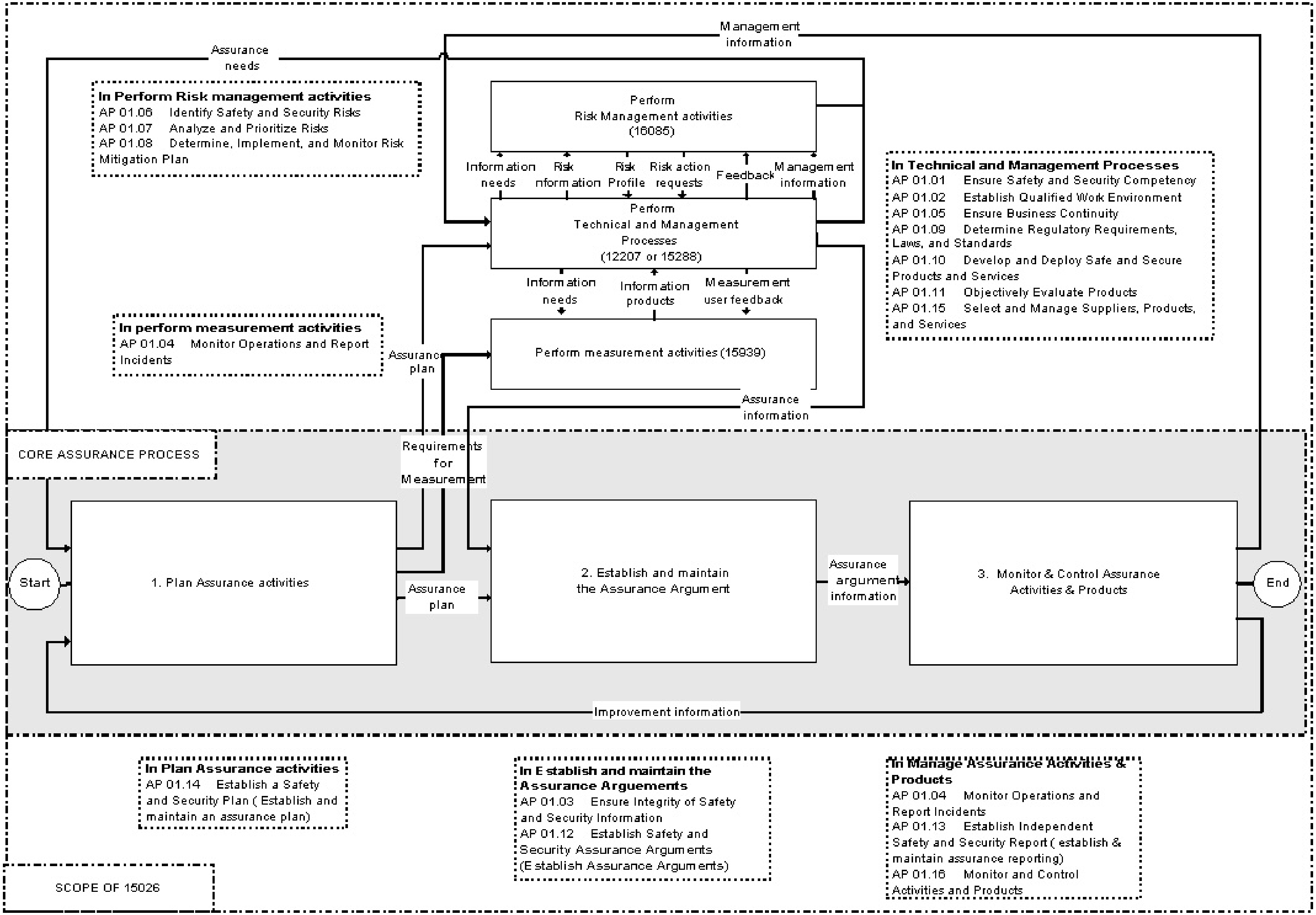
- Requirements
- Design
- V&V
- Test
- Risk Management
- Acquisition
- Architecture
-
-

Safety/Security Meta-Practices for ISO 15026*

1. Ensure Safety and Security Competency
2. Establish Qualified Work Environment
3. Ensure Integrity of Safety and Security Information
4. Monitor Operations and Report Incidents
5. Ensure Business Continuity
6. Identify Safety and Security Risks
7. Analyze and Prioritize Risks
8. Determine, Implement, and Monitor Risk Mitigation Plan
9. Determine Regulatory Requirements, Laws, and Standards
10. Develop and Deploy Safe and Secure Products and Services
11. Objectively Evaluate Products
12. Establish Safety and Security Assurance Arguments
13. Establish Independent Safety and Security Reporting
14. Establish a Safety and Security Plan
15. Select and Manage Suppliers, Products, and Services
16. Monitor and Control Activities and Products

Source: United States Federal Aviation Administration, www.faa.ipg,Safety and Security Extensions for Integrated Capability Maturity Models, September 2004

* Represents a synthesis/harmonization of 4 Security Standards with 4 Safety Standards


Management information
Assurance needs
Perform Risk Management activities (16085)
Information needs
Risk nformation
Risk Profile
Risk action requests
Feedback
Management information
Perform Technical and Management Processes (12207 or 15288)
Information needs
Information products
Measurement user feedback
Perform measurement activities (15939)
Assurance plan
Assurance information
CORE ASSURANCE PROCESS
Requirements for Measurement
Start
1. Plan Assurance activities
Assurance plan
2. Establish and maintain the Assurance Argument
Assurance argument information
3. Monitor & Control Assurance Activities & Products
End
Improvement information
SCOPE OF 15026

In Perform Risk management activities
AP 01.06 Identify Safety and Security Risks
AP 01.07 Analyze and Prioritize Risks
AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan

In Technical and Management Processes
AP 01.01 Ensure Safety and Security Competency
AP 01.02 Establish Qualified Work Environment
AP 01.05 Ensure Business Continuity
AP 01.09 Determine Regulatory Requirements, Laws, and Standards
AP 01.10 Develop and Deploy Safe and Secure Products and Services
AP 01.11 Objectively Evaluate Products
AP 01.15 Select and Manage Suppliers, Products, and Services

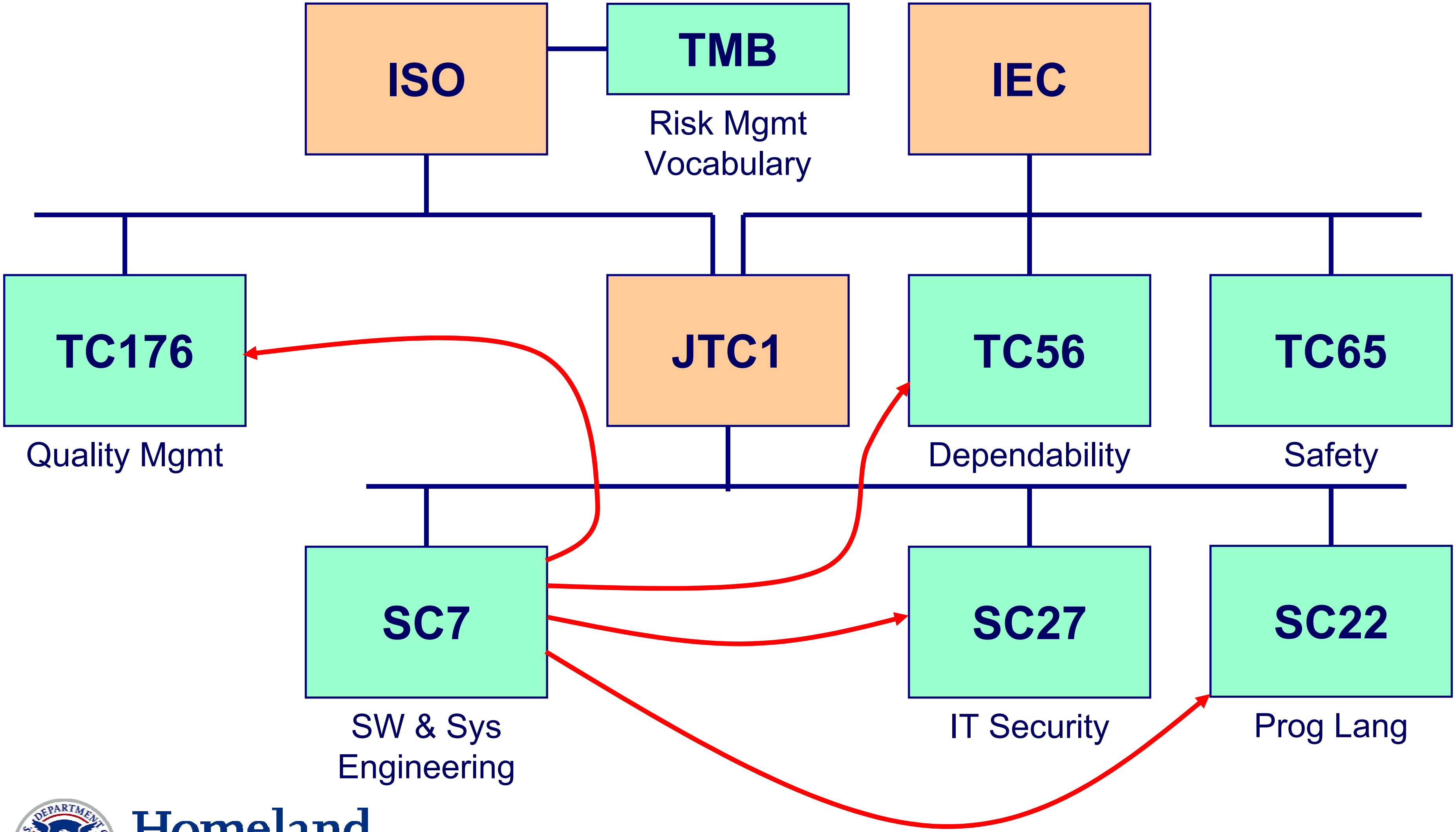
In perform measurement activities
AP 01.04 Monitor Operations and Report Incidents

In Plan Assurance activities
AP 01.14 Establish a Safety and Security Plan (Establish and maintain an assurance plan)

In Establish and maintain the Assurance Arguements
AP 01.03 Ensure Integrity of Safety and Security Information
AP 01.12 Establish Safety and Security Assurance Arguments (Establish Assurance Arguments)

In Manage Assurance Activities & Products
AP 01.04 Monitor Operations and Report Incidents
AP 01.13 Establish Independent Safety and Security Report (establish & maintain assurance reporting)
AP 01.16 Monitor and Control Activities and Products

Who are the Players? – International

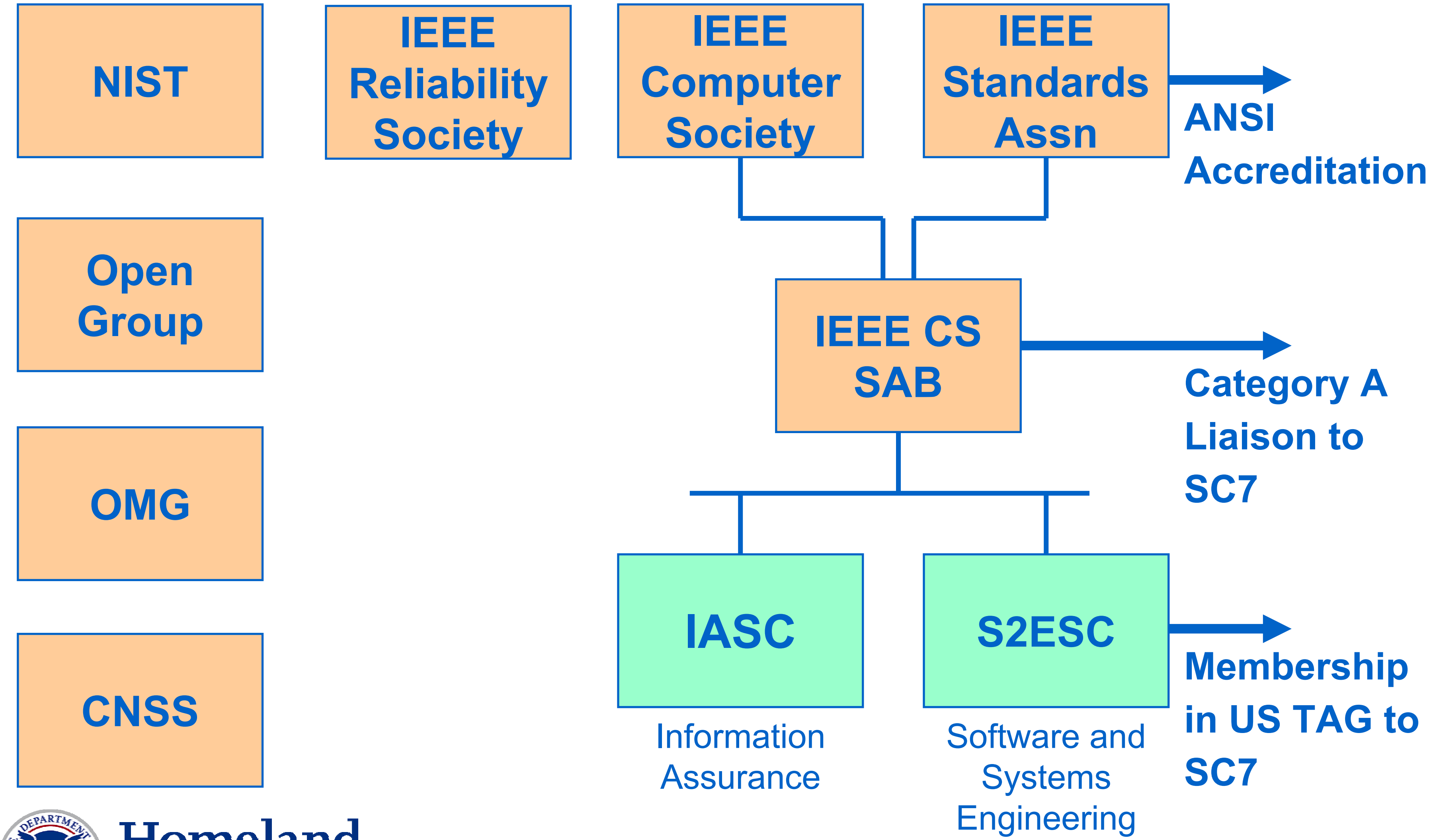


Homeland Security

INCITS CS1 Standardization Areas

- 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

Who are the Players? – in the US



NIST

IEEE Reliability Society

IEEE Computer Society

IEEE Standards Assn

ANSI Accreditation

Open Group

IEEE CS SAB

Category A Liaison to SC7

OMG

IASC

Information Assurance

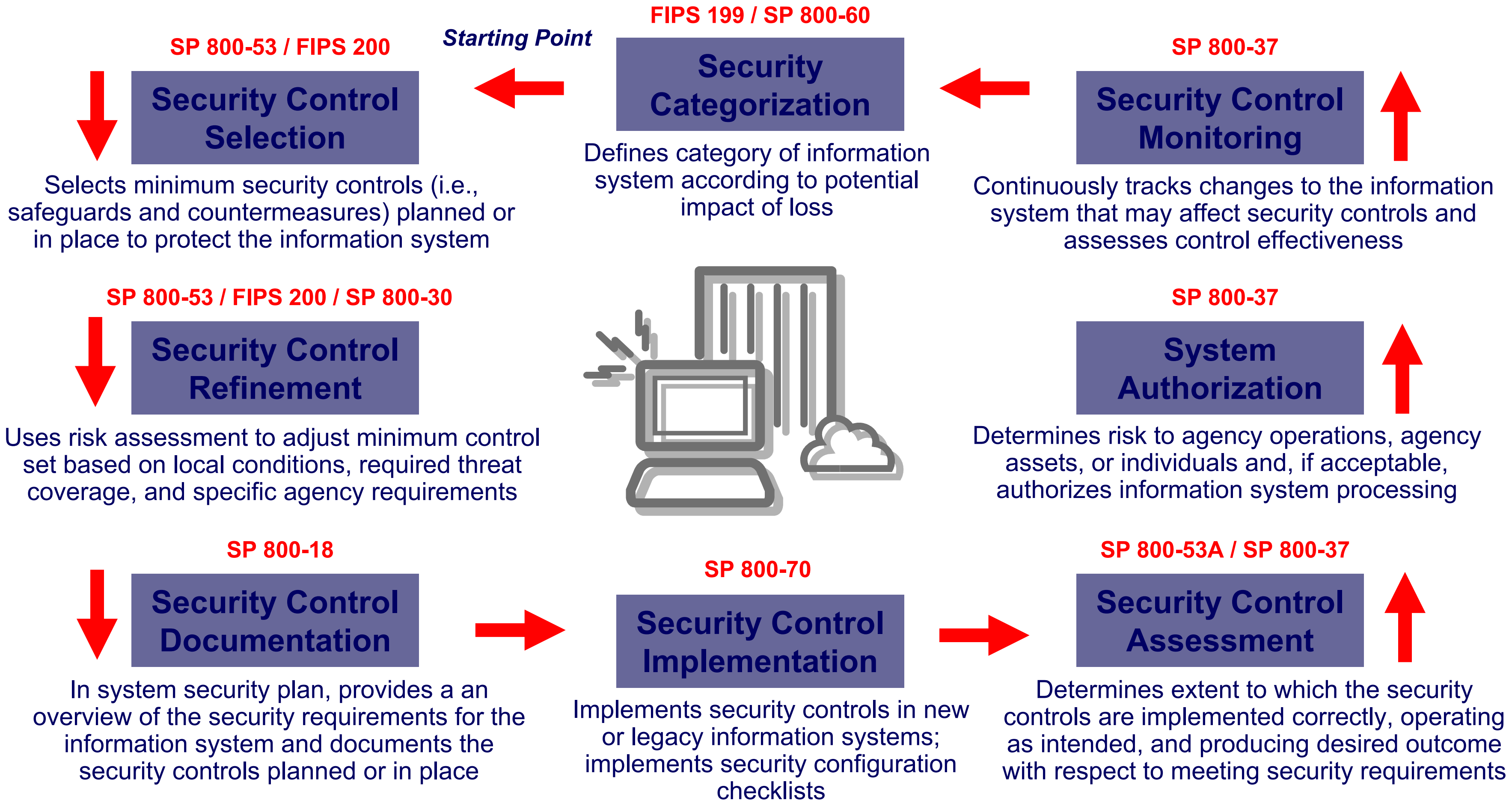
S2ESC

Software and Systems Engineering

Membership in US TAG to SC7

CNSS

NIST Enterprise Risk Management Framework



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

Starting Point

FIPS 199 / SP 800-60

Security Categorization

Defines category of information system according to potential impact of loss

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

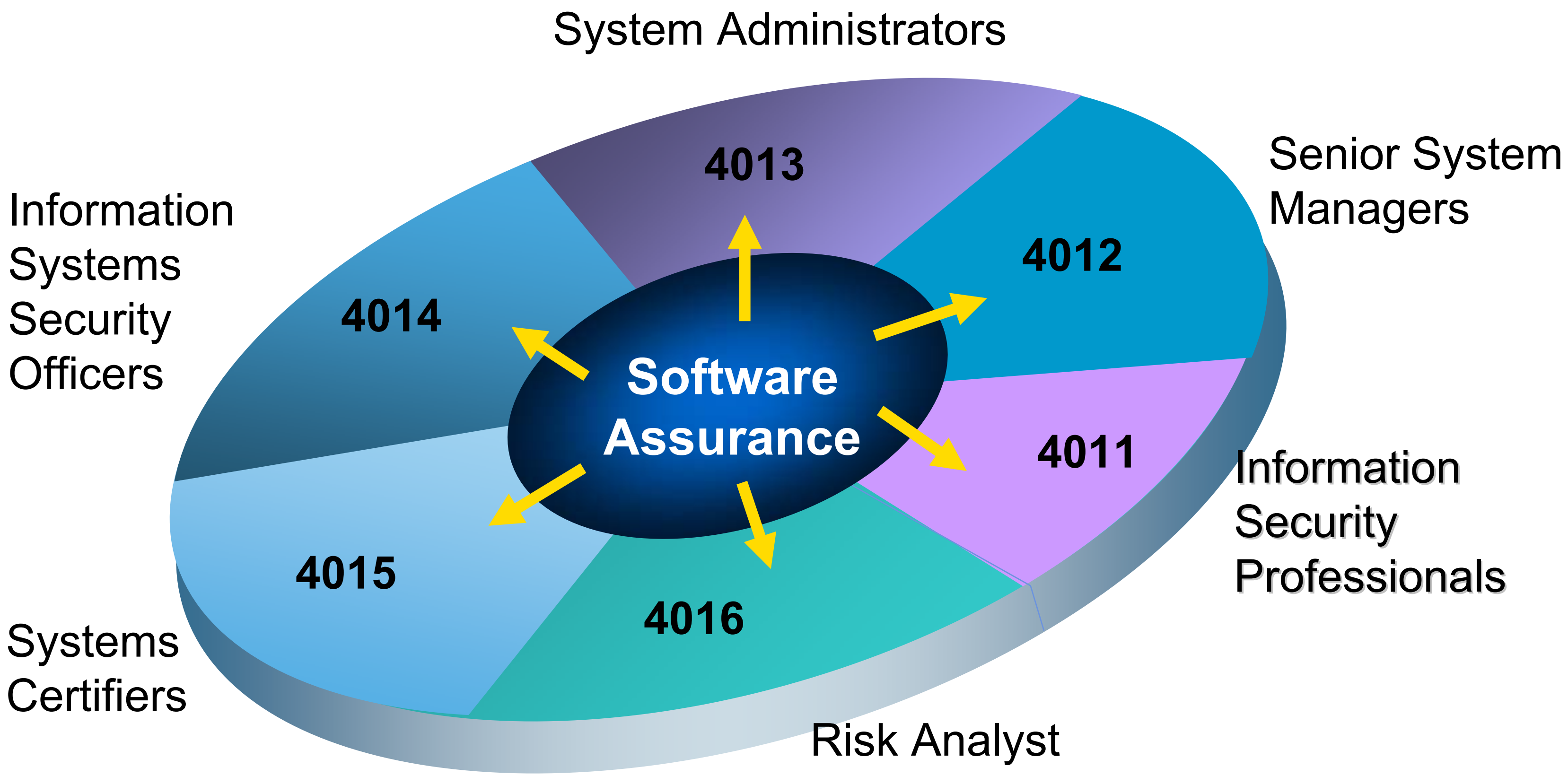
Source: FISMA Implementation Project, Dr. Ron Ross, NIST, April 2004

FISMA Implementation Project Standards and Guidelines

- FIPS Publication 199 (Security Categorization)
- NIST Special Publication 800-37 (Certification & Accreditation)
- NIST Special Publication 800-53 (Security Controls)
- NIST Special Publication 800-53A (Assessment)
- NIST Special Publication 800-59 (National Security)
- NIST Special Publication 800-60 (Category Mapping)
- FIPS Publication 200 (Minimum Security Controls)

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

Integrating SwA CBK with CNSS IA Standards



Software Assurance considerations for IA functional roles:

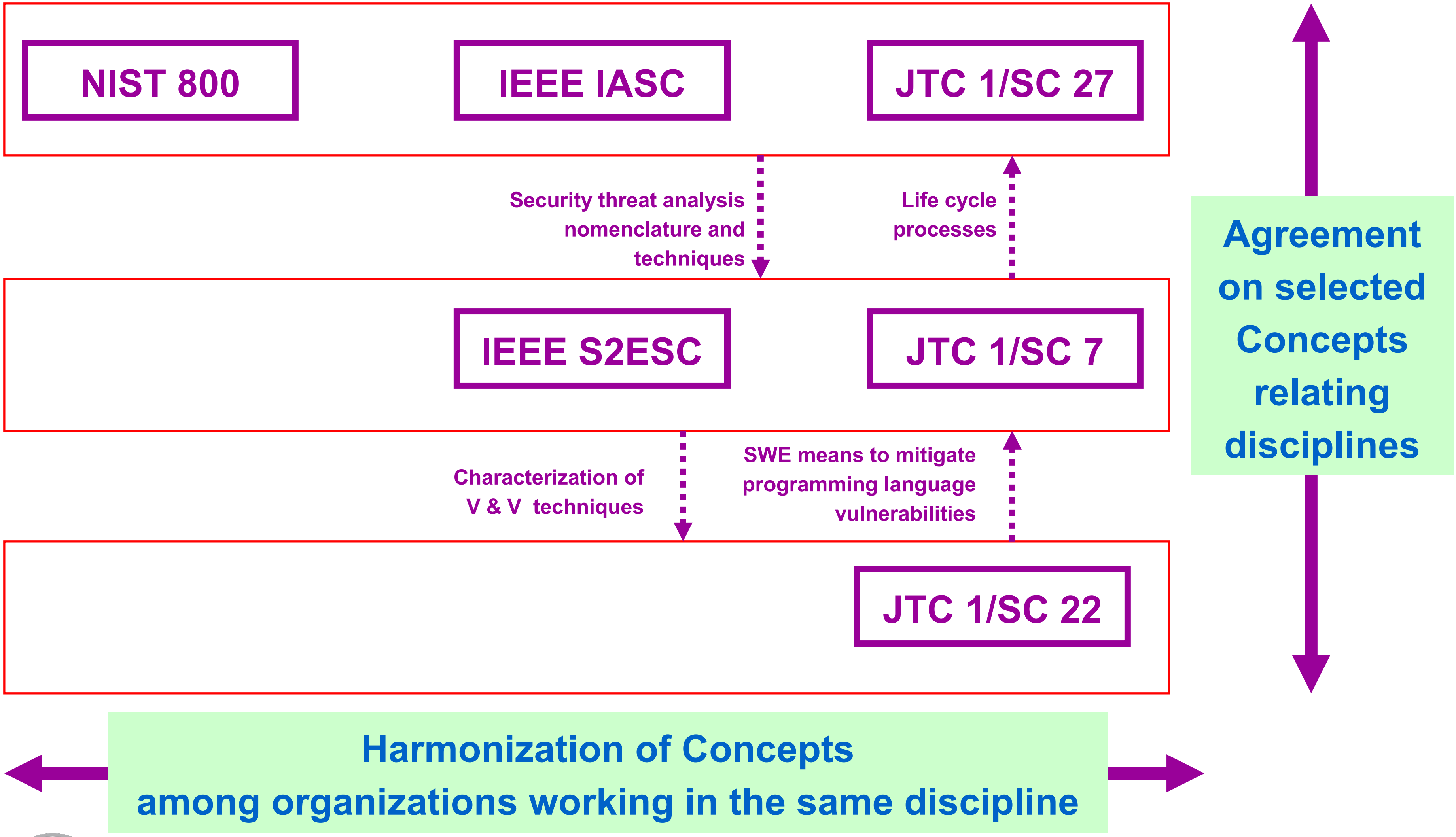
-- add SwA material in each CNSS 4000 series standard

-- add a new CNSS 4000 series standard on SW Assurance

Bottom Line

- The problem
  - A broad range of organizations
  - A broad range of technical committees
  - A broad range of standards and other documents that have developed more or less independently
- We need
  - Knowledgeable representation in the various committees of interest
  - A coordinated approach advocating convergence on the needs of SWA
- Recommended approach
  - Use subject matter experts as representatives to various committees
  - Achieve agreement on a set of concepts that can link the various standards
  - Work together to drive our committees toward the agreed concepts
  - Meet frequently to assess progress

Examples of Desired Relationships



NIST 800

IEEE IASC

JTC 1/SC 27

Security threat analysis nomenclature and techniques

Life cycle processes

IEEE S2ESC

JTC 1/SC 7

Characterization of V & V techniques

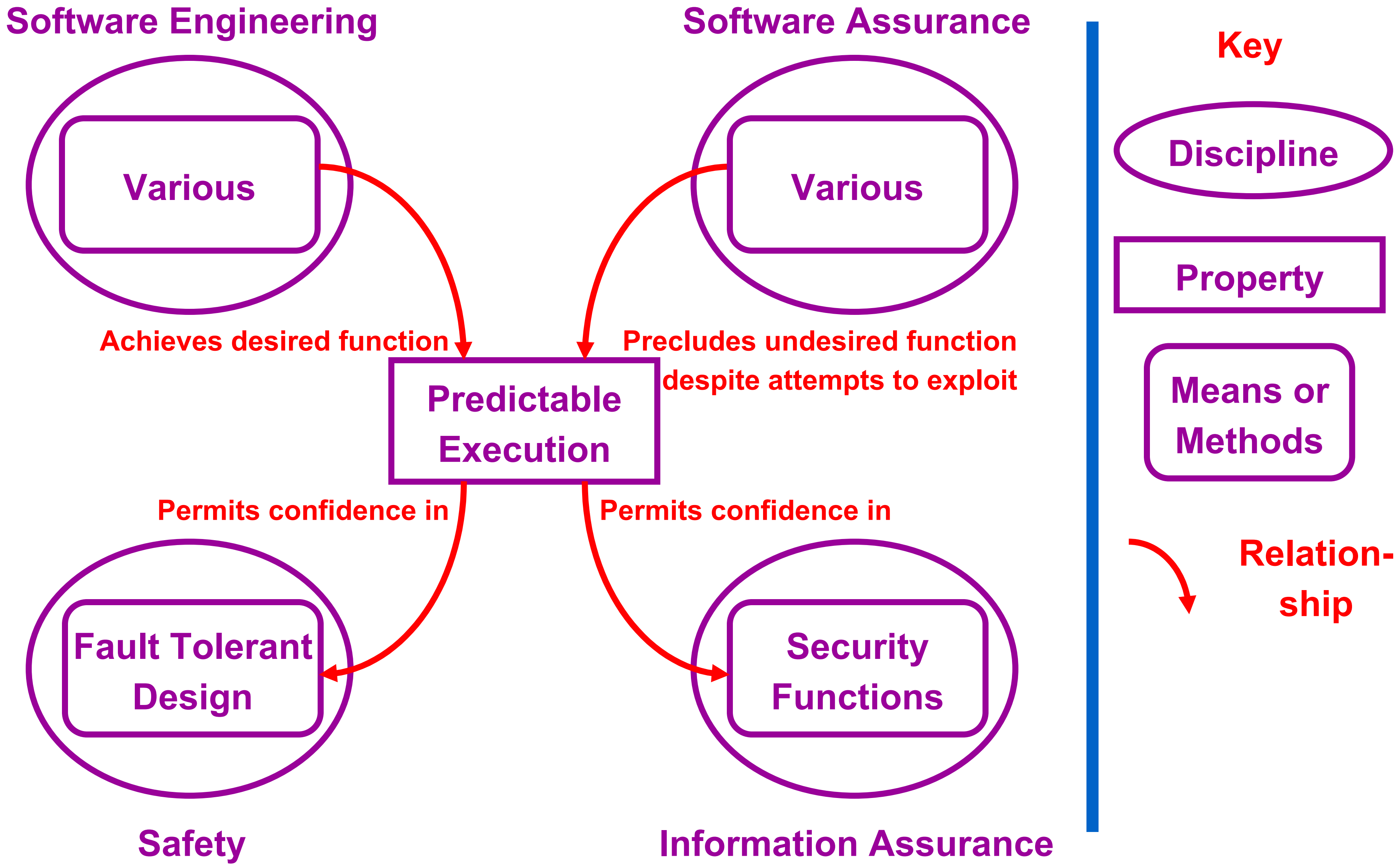
SWE means to mitigate programming language vulnerabilities

JTC 1/SC 22

Agreement on selected Concepts relating disciplines

Harmonization of Concepts among organizations working in the same discipline

(Over) Simplified Relationships among Disciplines



Possible Concepts from SW Engineering Standards

- A set of reference processes for describing the life cycle of software and systems
- Vocabulary related to software and systems
- Model for system and software measurement and process for doing so
- Model of product quality characteristics
- Generalized risk management process

Key Standards for Software and System Processes

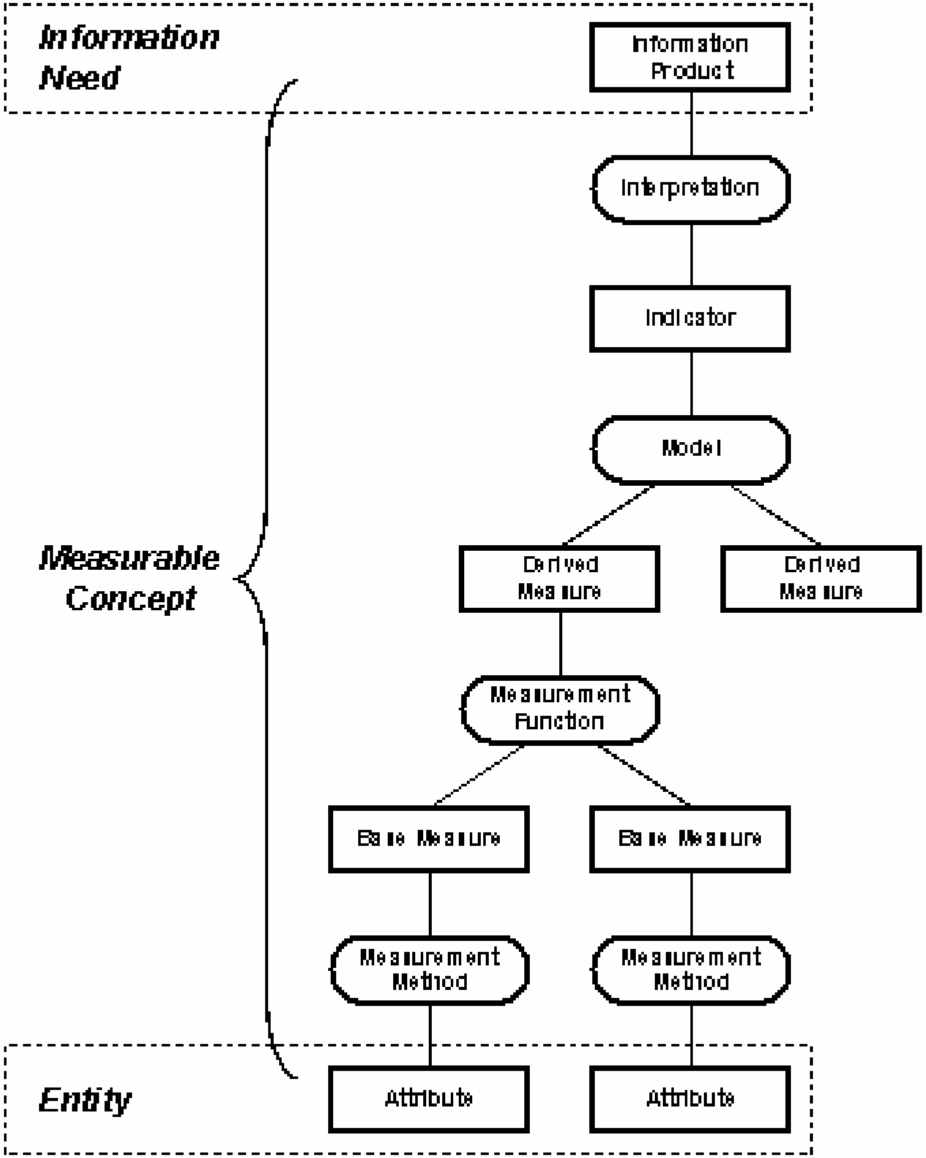
- ISO/IEC 15288, System Life Cycle Processes
  - 25 processes spanning the life cycle of a system.
  - The standard is primarily descriptive.
- ISO/IEC 12207:1995, Software Life Cycle Processes
  - 17 processes spanning the life cycle of a software product or service.
  - The standard is somewhat prescriptive in defining a minimum level of responsible practice.
  - Describes processes meeting the needs of organizational process definition.
- ISO/IEC 12207:Amd 1
  - Redescribes processes to meet the needs of process assessment and improvement.
- ISO/IEC 15026, Integrity Levels ➔ Assurance
  - Describes additional techniques needed for high-integrity systems.
  - Currently, not process-oriented, but is being repositioned.
- ISO/IEC 16085, Risk Management Process
- ISO/IEC 15939, Measurement Process
- Other standards treating specific processes in greater detail

Measurement Model

- IEEE adopted the measurement model of ISO/IEC 15389 …
- … which, in turn, came from the DoD Practical Software Measurement program.

http://standards.computer.org/sesc/sesc_pols

Homeland Security



Measurement Information Model

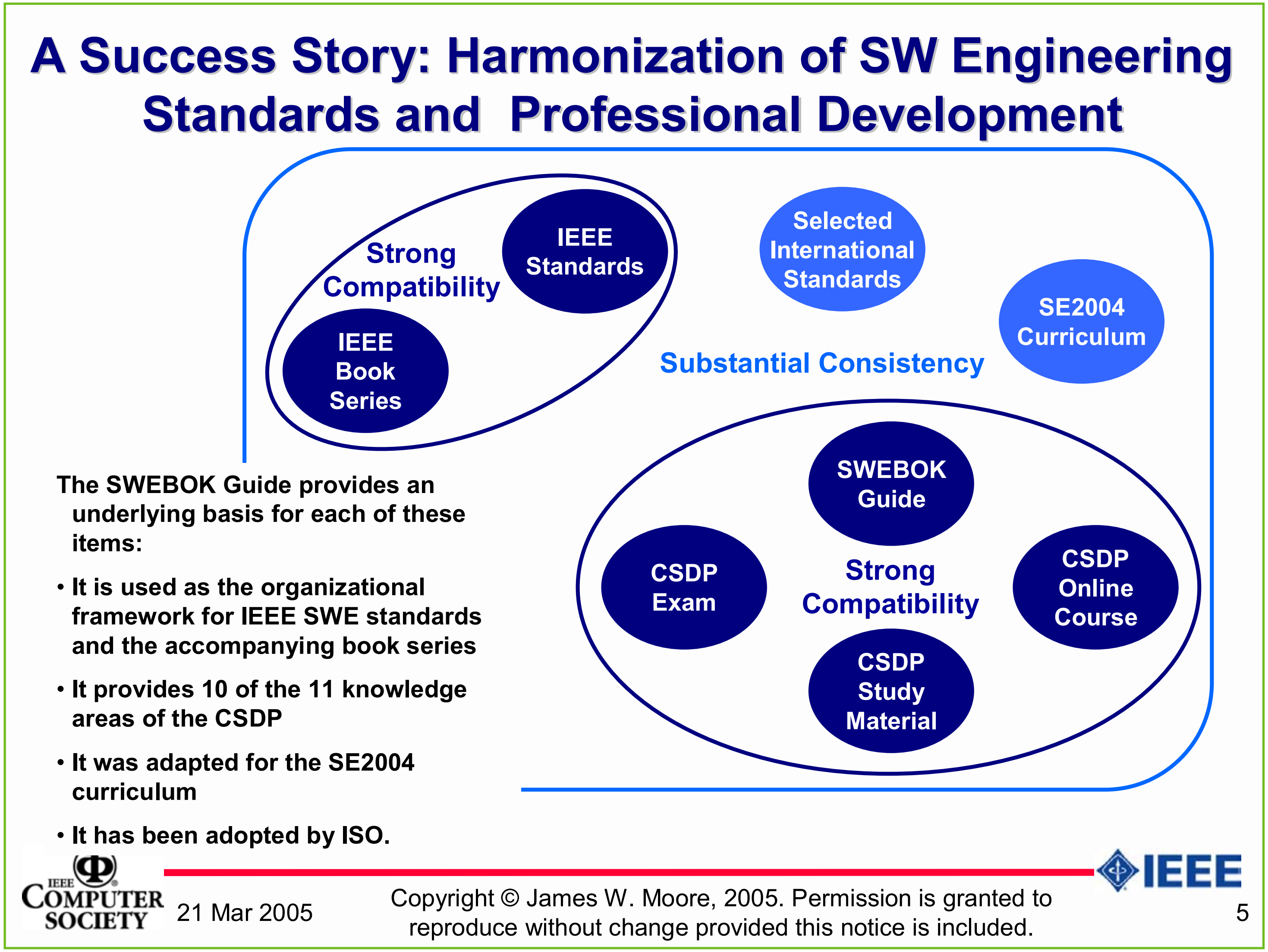
Vocabulary

- IEEE 610.12, Glossary of Software Engineering Terminology.
- JTC 1 doesn't have a system and software engineering vocabulary but does have a few near-misses of varying ages:
  - ISO/IEC 2382-1:1993, Information technology–Vocabulary–Part 1: Fundamental terms
  - ISO/IEC 2382-7:2000, Information technology–Vocabulary–Part 7: Computer programming
  - ISO/IEC 2382-8:1998, Information technology–Vocabulary–Part 8: Security
  - ISO/IEC 2382-14:1997, Information technology–Vocabulary–Part 14: Reliability, maintainability and availability
  - ISO/IEC 2382-20:1990, Information technology–Vocabulary–Part 20: System development

Some Current Efforts

- SC7
  - Incorporate “raise the floor” assurance practices into life cycle standards.
  - Incorporate “raise the ceiling” practices into separate standards strongly related to the life cycle standards.
  - Use “16 Practices” as a benchmark for measuring success.
- SC22
  - Develop coding guidelines for common programming languages.
- SC27
  - Expand their perceived context to include assurance concerns.
- IEEE S2ESC
  - Use as an “integrator” of standards for packaging and transition to industry.

Success of IEEE with this Strategy



A Success Story: Harmonization of SW Engineering Standards and Professional Development

Strong Compatibility

IEEE Standards

IEEE Book Series

Selected International Standards

SE2004 Curriculum

Substantial Consistency

SWEBOK Guide

CSDP Exam

Strong Compatibility

CSDP Online Course

CSDP Study Material

The SWEBOK Guide provides an underlying basis for each of these items:

- It is used as the organizational framework for IEEE SWE standards and the accompanying book series
- It provides 10 of the 11 knowledge areas of the CSDP
- It was adapted for the SE2004 curriculum
- It has been adopted by ISO.

IEEE COMPUTER SOCIETY 21 Mar 2005

IEEE

5

The success of the IEEE CS SWE harmonization happens to benefit the goals of software assurance.

It also provides a model for future efforts by software assurance.

Technology Transition Vehicles

- Professional Societies
  - Utilize professional societies as a source of expertise and as a mechanism for technology transition to individual practice.
- Body of Knowledge and Curriculum
  - Provide an authoritative overview of the knowledge needed by practitioners
  - Provide curriculum guidance for educators and industrial trainers
- Standards Infrastructure
  - Use standards as a mechanism for recording good software assurance practices and transitioning them to commercial usage.
  - Provide named benchmarks for use in contracting, license agreements, insurance ratings, etc.
- Product Assessment
  - Provide a framework for assessing the security and assurance characteristics of products and providing appropriate product certifications, e.g. NIAP and improvements.
- Organizational Assessment
  - Provide a framework for assessing the capability of an organization to develop and sustain products demonstrating desired characteristics of software assurance, e.g. CMMI (and iCMM) supplemented by “Sixteen Practices” for software assurance
- Critical Infrastructure Applications
  - Provide technologies, practices, standards and guidance for incorporating assurance practices into products and services applied to critical infrastructure.

Software Assurance: Acquisition

- Enhance software supply chain management through improved risk mitigation and contracting for secure software**
    - Collaborate with CNSS and industry working groups to identify needs for reducing risks associated with software supply chain
    - Develop and disseminate templates for acquisition language and evaluation based on successful models
    - Develop and disseminate common or sample statement of work / procurement language that includes provisions on liability for federal acquisition managers
    - Provide materials to organizations providing acquisition training and education

**NCSD Goal Action 2.3.4

Software Assurance: Technology

- Enhance software security measurement and assess Software Assurance testing and diagnostic tools**
  - Collaborate with National Institute of Standards and Technology (NIST) to inventory software assurance tools and measure effectiveness, identify gaps and conflicts, and develop a plan to eliminate gaps and conflicts
    - Host workshops with NIST to assess, measure, and validate tool effectiveness
  - Develop R&D requirements for DHS S&T consideration; coordinating Software Assurance R&D requirements with other federal agencies
    - Fund a R&D project (through the DHS S&T Directorate) that will examine tools and techniques for analyzing software to detect security vulnerabilities.
    - Include techniques that require access to source code, as well as binary-only techniques
  - Collaborate with other agencies and allied organizations to mature measurement in security

**NCSD Goal Action 2.3.3

Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of Standards and Technology

National Vulnerability Database

a comprehensive cyber vulnerability resource

The National Vulnerability Database (NVD) is new vulnerability resource tool co-sponsored by NIST and the DHS National Cyber Security Division/US-CERT, and:

- Is a comprehensive IT vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides links to industry resources
- Is built upon the CVE standard vulnerability nomenclature and augments the standard with a search engine and reference library
- Provides IT professionals with centralized and comprehensive vulnerability information in order to assist with incident prevention and management to mitigate the impact of vulnerabilities
- Strives to include all industry vulnerability databases, creating a “meta search engine”
- Provides official U.S. Government information on virtually all vulnerabilities
- Provides a fine grained search capability
- Provides user requested vulnerability statistics

Homeland Security

http://nvd.nist.gov

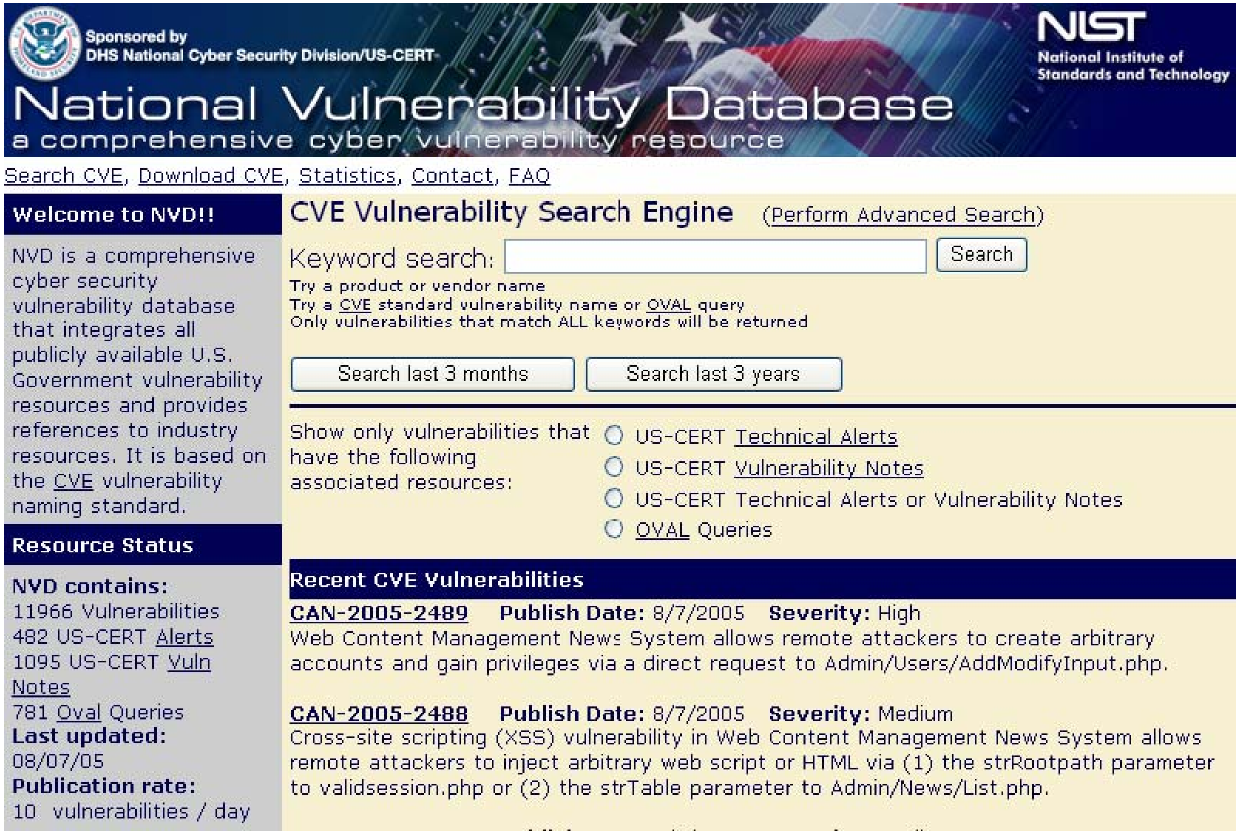
NVD Search Capability

The NVD enables users to search a database containing virtually all known public computer vulnerabilities by a variety of vulnerability characteristics including:

- related exploit range
- vendor name
- software name and version number
- vulnerability type, severity, impact

Updated every 4 minutes, to date, the NVD contains:

- Over 12,000 vulnerability summaries
- 482 US-CERT Advisories
- 1095 US-CERT Vulnerability Notes
- 781 OVAL references
- 47,000 industry references
- 36 executable Cold Fusion programs


Sponsored by
DHS National Cyber Security Division/US-CERT
NIST
National Institute of Standards and Technology
National Vulnerability Database
a comprehensive cyber vulnerability resource
Search CVE, Download CVE, Statistics, Contact, FAQ
Search
Search last 3 months
Search last 3 years

Welcome to NVD!!

NVD is a comprehensive cyber security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources. It is based on the CVE vulnerability naming standard.

Resource Status

NVD contains:
11966 Vulnerabilities
482 US-CERT Alerts
1095 US-CERT Vuln Notes
781 Oval Queries
Last updated:
08/07/05
Publication rate:
10 vulnerabilities / day

CVE Vulnerability Search Engine (Perform Advanced Search)

Keyword search:

Try a product or vendor name
Try a CVE standard vulnerability name or OVAL query
Only vulnerabilities that match ALL keywords will be returned

Show only vulnerabilities that have the following associated resources:

○ US-CERT Technical Alerts
○ US-CERT Vulnerability Notes
○ US-CERT Technical Alerts or Vulnerability Notes
○ OVAL Queries

Recent CVE Vulnerabilities

CAN-2005-2489 **Publish Date:** 8/7/2005 **Severity:** High
Web Content Management News System allows remote attackers to create arbitrary accounts and gain privileges via a direct request to Admin/Users/AddModifyInput.php.

CAN-2005-2488 **Publish Date:** 8/7/2005 **Severity:** Medium
Cross-site scripting (XSS) vulnerability in Web Content Management News System allows remote attackers to inject arbitrary web script or HTML via (1) the strRootpath parameter to validsession.php or (2) the strTable parameter to Admin/News/List.php.

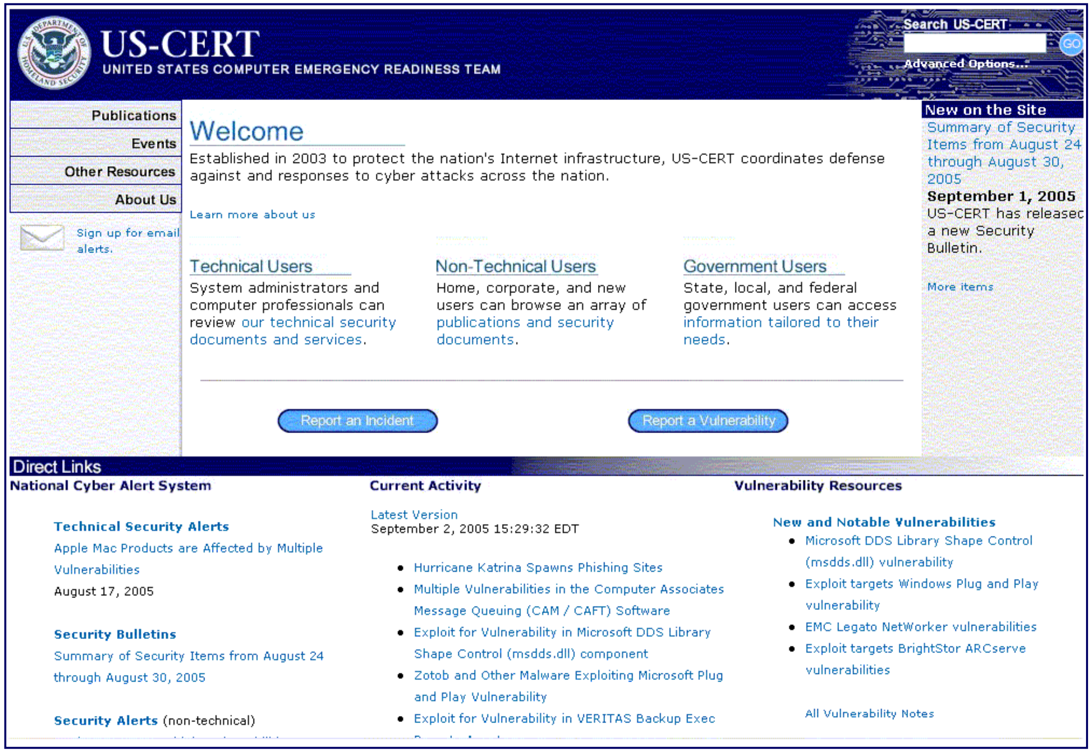
http://nvd.nist.gov

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
- Pivotal momentum gathering in recognition of (and commitment to) process improvement in acquisition, management and engineering
  - Synergy of good ideas and resources will continue to be key ingredient
  - Security requirements need to be addressed along with other functions
- 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, Federal agencies need to focus on software assurance as a means of better enabling operational resiliency

Homeland Security

www.us-cert.gov



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Welcome

Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation.

Learn more about us

Technical Users
System administrators and computer professionals can review our technical security documents and services.

Non-Technical Users
Home, corporate, and new users can browse an array of publications and security documents.

Government Users
State, local, and federal government users can access information tailored to their needs.

New on the Site
Summary of Security Items from August 24 through August 30, 2005
September 1, 2005
US-CERT has releasec a new Security Bulletin.
More items

Direct Links

National Cyber Alert System

Technical Security Alerts
Apple Mac Products are Affected by Multiple Vulnerabilities
August 17, 2005

Security Bulletins
Summary of Security Items from August 24 through August 30, 2005

Security Alerts (non-technical)

Current Activity

Latest Version
September 2, 2005 15:29:32 EDT

- Hurricane Katrina Spawns Phishing Sites
- Multiple Vulnerabilities in the Computer Associates Message Queuing (CAM / CAFT) Software
- Exploit for Vulnerability in Microsoft DDS Library Shape Control (msdds.dll) component
- Zotob and Other Malware Exploiting Microsoft Plug and Play Vulnerability
- Exploit for Vulnerability in VERITAS Backup Exec

Vulnerability Resources

New and Notable Vulnerabilities

- Microsoft DDS Library Shape Control (msdds.dll) vulnerability
- Exploit targets Windows Plug and Play vulnerability
- EMC Legato NetWorker vulnerabilities
- Exploit targets BrightStor ARCserve vulnerabilities

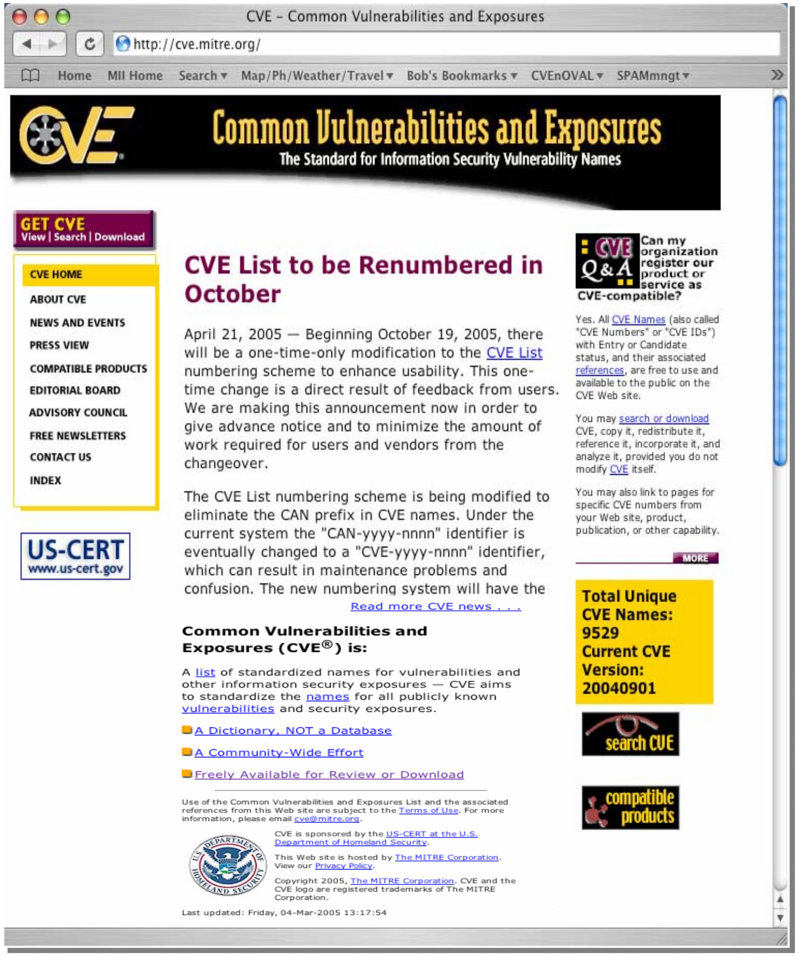
All Vulnerability Notes

Joe Jarzombek, PMP
Director for Software Assurance
National Cyber Security Division (NCSD)
Information Analysis and Infrastructure Protection (IAIP)
U.S. Department of Homeland Security
Joe.Jarzombek@dhs.gov
(703) 235-5126

Back-up Slides

Common Vulnerabilities and Exposures (CVE) Initiative

- An international security community activity
  - to provide common names for publicly known security vulnerabilities and exposures
- Key tenets
  - One name for one vulnerability or exposure
  - One standardized description for each
  - Existence as a dictionary
  - Publicly accessible on the Internet
  - Industry participation in open forum (editorial board)
- The CVE list and information at [cve.mitre.org]



Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

CVE List to be Renumbered in October

April 21, 2005 — Beginning October 19, 2005, there will be a one-time-only modification to the CVE List numbering scheme to enhance usability. This one-time change is a direct result of feedback from users. We are making this announcement now in order to give advance notice and to minimize the amount of work required for users and vendors from the changeover.

The CVE List numbering scheme is being modified to eliminate the CAN prefix in CVE names. Under the current system the "CAN-yyyy-nnnn" identifier is eventually changed to a "CVE-yyyy-nnnn" identifier, which can result in maintenance problems and confusion. The new numbering system will have the

Read more CVE news . . .

Common Vulnerabilities and Exposures (CVE®) is:

A list of standardized names for vulnerabilities and other information security exposures — CVE aims to standardize the names for all publicly known vulnerabilities and security exposures.

- A Dictionary, NOT a Database
- A Community-Wide Effort
- Freely Available for Review or Download

Use of the Common Vulnerabilities and Exposures List and the associated references from this Web site are subject to the Terms of Use. For more information, please email cve@mitre.org.

CVE is sponsored by the US-CERT at the U.S. Department of Homeland Security.

This Web site is hosted by The MITRE Corporation. View our Privacy Policy.

Copyright 2005, The MITRE Corporation. CVE and the CVE logo are registered trademarks of The MITRE Corporation.

Last updated: Friday, 04-Mar-2005 13:17:54

Can my organization register our product or service as CVE-compatible?

Yes. All CVE Names (also called "CVE Numbers" or "CVE IDs") with Entry or Candidate status, and their associated references, are free to use and available to the public on the CVE Web site.

You may search or download CVE, copy it, redistribute it, reference it, incorporate it, and analyze it, provided you do not modify CVE itself.

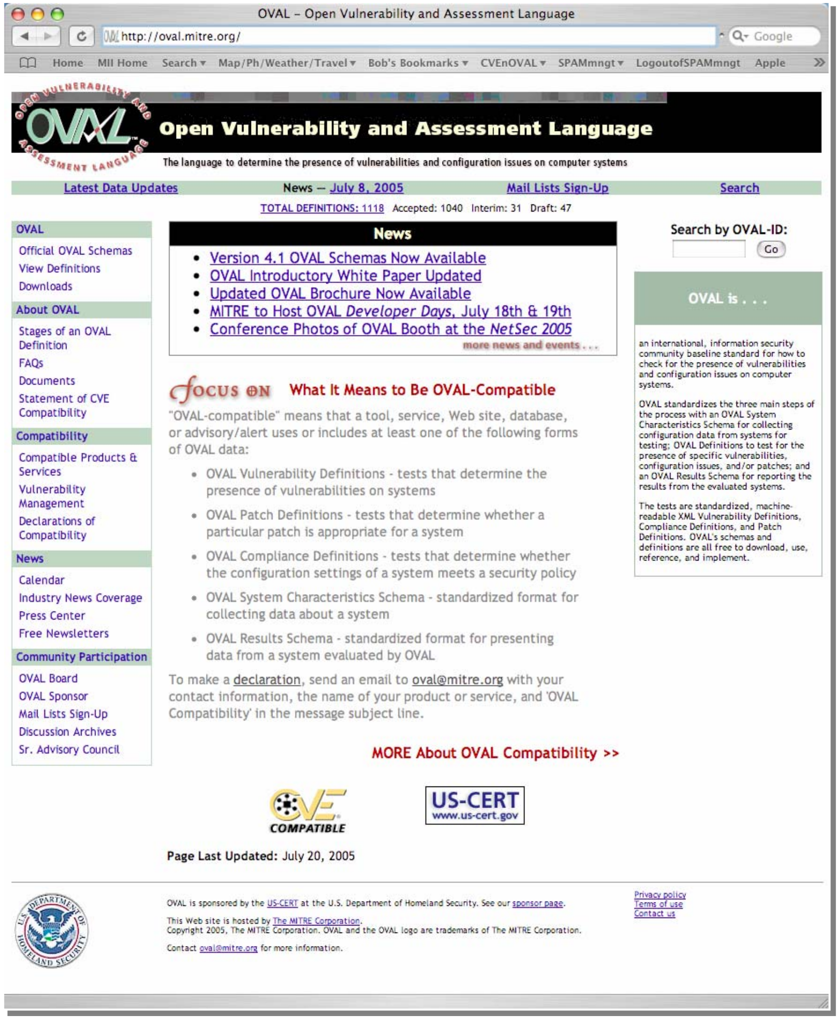
You may also link to pages for specific CVE numbers from your Web site, product, publication, or other capability.

Total Unique CVE Names: 9529
Current CVE Version: 20040901

12,081 unique CVE names ~350-500 new/month

OVAL Concept
- The Open Vulnerability and Assessment Language Initiative

- Community-based collaboration
- Precise definitions to test for each vulnerability, misconfiguration, policy, or patch
- Standard schema of security-relevant configuration information
- OVAL schema and definitions freely available for download, public review, and comment
- Security community suggests new definitions and schema
- OVAL board considers proposed schema modifications



Open Vulnerability and Assessment Language

The language to determine the presence of vulnerabilities and configuration issues on computer systems

Latest Data Updates | News — July 8, 2005 | Mail Lists Sign-Up | Search

TOTAL DEFINITIONS: 1118 Accepted: 1040 Interim: 31 Draft: 47

OVAL
Official OVAL Schemas
View Definitions
Downloads

About OVAL
Stages of an OVAL Definition
FAQs
Documents
Statement of CVE Compatibility

Compatibility
Compatible Products & Services
Vulnerability Management
Declarations of Compatibility

News
Calendar
Industry News Coverage
Press Center
Free Newsletters

Community Participation
OVAL Board
OVAL Sponsor
Mail Lists Sign-Up
Discussion Archives
Sr. Advisory Council

News
- Version 4.1 OVAL Schemas Now Available
- OVAL Introductory White Paper Updated
- Updated OVAL Brochure Now Available
- MITRE to Host OVAL *Developer Days*, July 18th & 19th
- Conference Photos of OVAL Booth at the *NetSec 2005*

more news and events . . .

Focus ON **What It Means to Be OVAL-Compatible**

"OVAL-compatible" means that a tool, service, Web site, database, or advisory/alert uses or includes at least one of the following forms of OVAL data:

- OVAL Vulnerability Definitions - tests that determine the presence of vulnerabilities on systems
- OVAL Patch Definitions - tests that determine whether a particular patch is appropriate for a system
- OVAL Compliance Definitions - tests that determine whether the configuration settings of a system meets a security policy
- OVAL System Characteristics Schema - standardized format for collecting data about a system
- OVAL Results Schema - standardized format for presenting data from a system evaluated by OVAL

To make a declaration, send an email to oval@mitre.org with your contact information, the name of your product or service, and 'OVAL Compatibility' in the message subject line.

MORE About OVAL Compatibility >>

CVE COMPATIBLE

US-CERT
www.us-cert.gov

Page Last Updated: July 20, 2005

Search by OVAL-ID:
Go

OVAL is . . .

an international, information security community baseline standard for how to check for the presence of vulnerabilities and configuration issues on computer systems.

OVAL standardizes the three main steps of the process with an OVAL System Characteristics Schema for collecting configuration data from systems for testing; OVAL Definitions to test for the presence of specific vulnerabilities, configuration issues, and/or patches; and an OVAL Results Schema for reporting the results from the evaluated systems.

The tests are standardized, machine-readable XML Vulnerability Definitions, Compliance Definitions, and Patch Definitions. OVAL's schemas and definitions are all free to download, use, reference, and implement.

OVAL is sponsored by the US-CERT at the U.S. Department of Homeland Security. See our sponsor page.

This Web site is hosted by The MITRE Corporation.
Copyright 2005, The MITRE Corporation. OVAL and the OVAL logo are trademarks of The MITRE Corporation.

Contact oval@mitre.org for more information.

Privacy policy
Terms of use
Contact us

1,141 OVAL Definitions

http://oval.mitre.org

Public unveiling - December 2002

Common Malware Enumeration (CME) Initiative

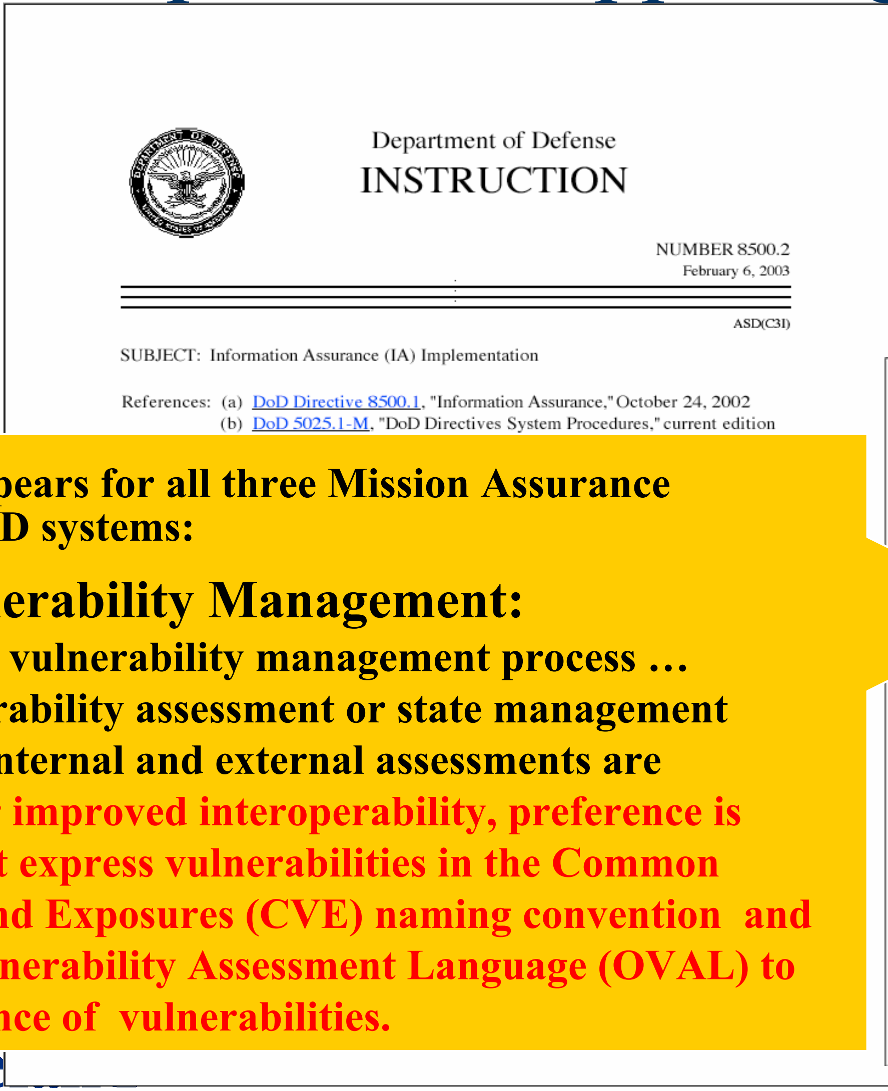
"For those of your customers that use more than one companies anti-virus product, … [the lack of common identifiers] left them with an even bigger mess than just the virus outbreak…. We should not have to work so hard to figure out if your products are keeping us protected."

-Chris Mosby, SMS Administrator, open letter posted to SANS Internet Storm Center and directed toward Anti-Virus companies.

- Assign unique IDs to high profile malware threats
- Create a community forum for sample exchange and deconfliction
- Standardize malware analysis content to provide consistent information to incident responders and enable machine consumption by network management tools

Building on CVE and OVAL efforts

DoD 8500.2 IA Implementation Instruction gives *preference* to products supporting CVE & OVAL



Department of Defense
INSTRUCTION

NUMBER 8500.2
February 6, 2003

ASD(C3I)

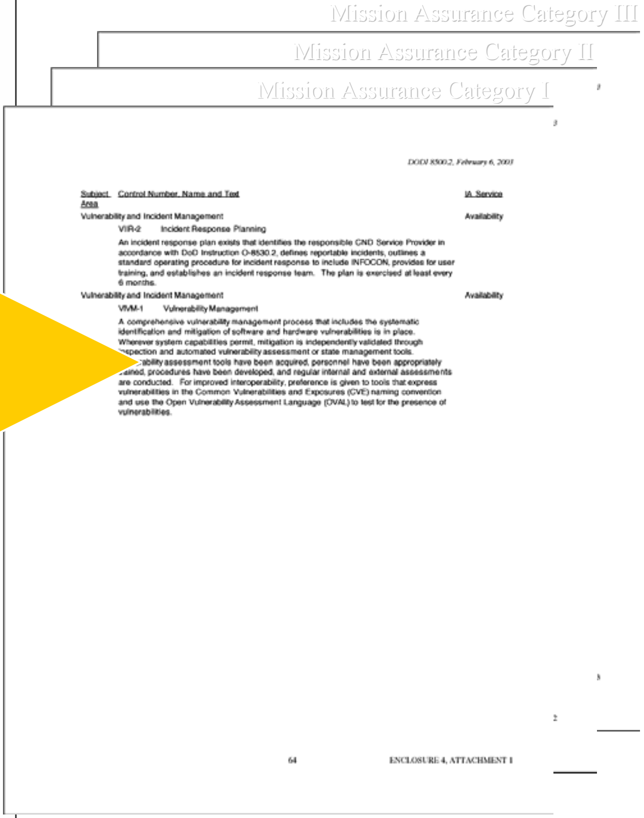
SUBJECT: Information Assurance (IA) Implementation

References: (a) DoD Directive 8500.1, "Information Assurance," October 24, 2002
(b) DoD 5025.1-M, "DoD Directives System Procedures," current edition

The following appears for all three Mission Assurance Categories of DOD systems:

VIVM-1 Vulnerability Management:

A comprehensive vulnerability management process … automated vulnerability assessment or state management tools … regular internal and external assessments are conducted … For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.



Mission Assurance Category III

Mission Assurance Category II

Mission Assurance Category I

DODI 8500.2, February 6, 2003

Subject Area	Control Number, Name and Text	IA Service
Vulnerability and Incident Management		Availability
	VIR-2 Incident Response Planning	
	An incident response plan exists that identifies the responsible CND Service Provider in accordance with DoD Instruction O-8530.2, defines reportable incidents, outlines a standard operating procedure for incident response to include INFOCON, provides for user training, and establishes an incident response team. The plan is exercised at least every 6 months.	
Vulnerability and Incident Management		Availability
	VIVM-1 Vulnerability Management	
	A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place. Wherever system capabilities permit, mitigation is independently validated through inspection and automated vulnerability assessment or state management tools. …ability assessment tools have been acquired, personnel have been appropriately …ained, procedures have been developed, and regular internal and external assessments are conducted. For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.	

64 ENCLOSURE 4, ATTACHMENT 1

http://www.nstissc.gov/html/library.htm

CVE Editorial Board

MITRE

Sun microsystems

NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA

CITADEL SECURITY SOFTWARE

IBM®

Microsoft®

U.S. Department of Energy CIAC Computer Incident Advisory Center

INTRANODE SOFTWARE TECHNOLOGIES

redhat.

symantec.™

Cisco Systems

EWA

nCircle NETWORK SECURITY

Nessus

NTBUGTRAQ

DEFENSE INFORMATION SYSTEMS AGENCY GNOSC GLOBAL NETWORK OPERATIONS & SECURITY CENTER

UCDAVIS

BIND VIEW

NIST National Institute of Standards and Technology

NFR SECURITY

STAT SECURITY THREAT AVOIDANCE TECHNOLOGY

Carnegie Mellon Software Engineering Institute

CERIAS Center for Education and Research in Information Assurance and Security

SANS INSTITUTE

INTERNET SECURITY SYSTEMS

SILICON DEFENSE

ca Computer Associates®

l ity

security-focus.com

GENERAL DYNAMICS Advanced Information Systems

GUARDEDNET

OVAL Board

redhat.

IBM®

CERIAS
Center for Education and Research
in Information Assurance and Security

netIQ®
Work Smarter.

Cisco Systems ®

debian

SANS
INSTITUTE

desktopstandard

e

QuickTi… and a
TIFF (Uncompressed) decompress
are needed to see this picture.

HARRIS

THE CENTER FOR
INTERNET SECURITY℠

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

INTERNET
SECURITY
SYSTEMS

Bastille Linux

CSC

symantec.

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

MITRE

QUALYS™

BIND VIEW

Carnegie Mellon
Software Engineering Institute

Microsoft®

DEFENSE INFORMATION SYSTEMS AGENCY

nCircle°
NETWORK SECURITY

ırity

ArcSight

CITADEL
SECURITY SOFTWARE

secure elements
enterprise vulnerability management

GUARDEDNET

CME Preliminary Advisory Board
A partnership with industry

- Established CME Preliminary Editorial Board (CME-PEB) with top thought leaders in AV industry
- Gained agreement regarding membership and identifier assignment processes

McAfee

TREND MICRO

symantec.

KASPERSKY lab

Microsoft

NORMAN

MessageLabs

F-SECURE

ca Computer Associates

Represents over 80% of world-wide market share as reported by IDC: Symantec (40.4%), McAfee (20.5%), Trend Micro (14.2%)

Any network disruption can be detrimental to the critical infrastructure

- Disruptions include cyber threats such as:
  - Viruses and worms
  - Trojans and bots
  - Identity theft

Examples of Losses and Damages

Love Bug:
$15B in damages
3.9M systems Infected/30 days to clean up
2000

Code Red:
$1.2B in damages
$740M to clean up
the 360,000 infected servers
2001

Slammer:
$1B in damages

2002

Blaster:
$50B in damages

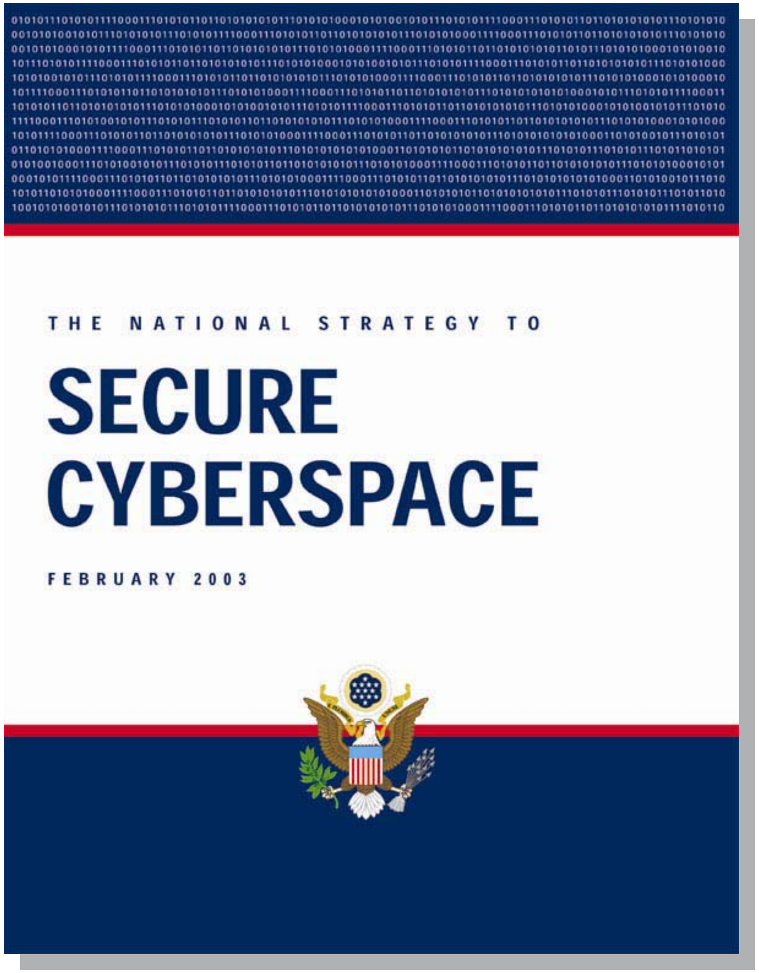
2003

My Doom:
$38B in damages
Worldwide

2004

- System hacking affects national security and economy
- Concern about growth in use of malicious code, such as spyware

National Strategy – Five Priorities



THE NATIONAL STRATEGY TO

SECURE CYBERSPACE

FEBRUARY 2003

- National Cyberspace Response System
- National Cyberspace Threat and Vulnerability Reduction Program
- National Cyberspace Security Awareness and Training Program
- Securing Government's Cyberspace
- International Cyberspace Security Cooperation

The National Strategy to Secure Cyberspace

> “In the past few years, threats in cyberspace have risen dramatically. The policy of the United States is to protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States. We must act to reduce our vulnerabilities to these threats before they can be exploited to damage the cyber systems supporting our Nation’s critical infrastructures and ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable, and cause the least damage possible.”

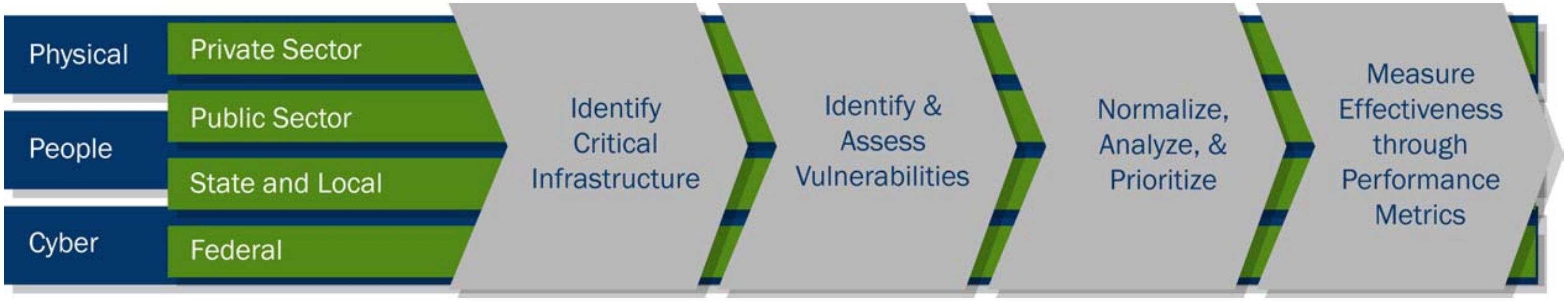
President George W. Bush

February, 2003

The National Infrastructure Protection Plan (NIPP) outlines a unifying structure

- Allows all levels of government to collaborate with the appropriate private sector entities
- Encourages the development of information sharing and analysis mechanisms and continues to support existing sector-coordinating mechanisms
- Broken down into 17 sector-specific plans to cover all areas of critical infrastructure, including the Information Technology sector

NIPP Risk Management Framework


Physical
People
Cyber
Private Sector
Public Sector
State and Local
Federal
Identify Critical Infrastructure
Identify & Assess Vulnerabilities
Normalize, Analyze, & Prioritize
Measure Effectiveness through Performance Metrics

NCSD goals are strategically aligned with the *National Strategy to Secure Cyberspace & HSPD-7 & NIPP*

NATIONAL STRATEGY PRIORITIES

I. National Cyberspace Security Response System

II. National Cyberspace Threat and Vulnerability Reduction Program

III. National Cyberspace Security Awareness and Training Program

IV. Securing Governments Cyberspace

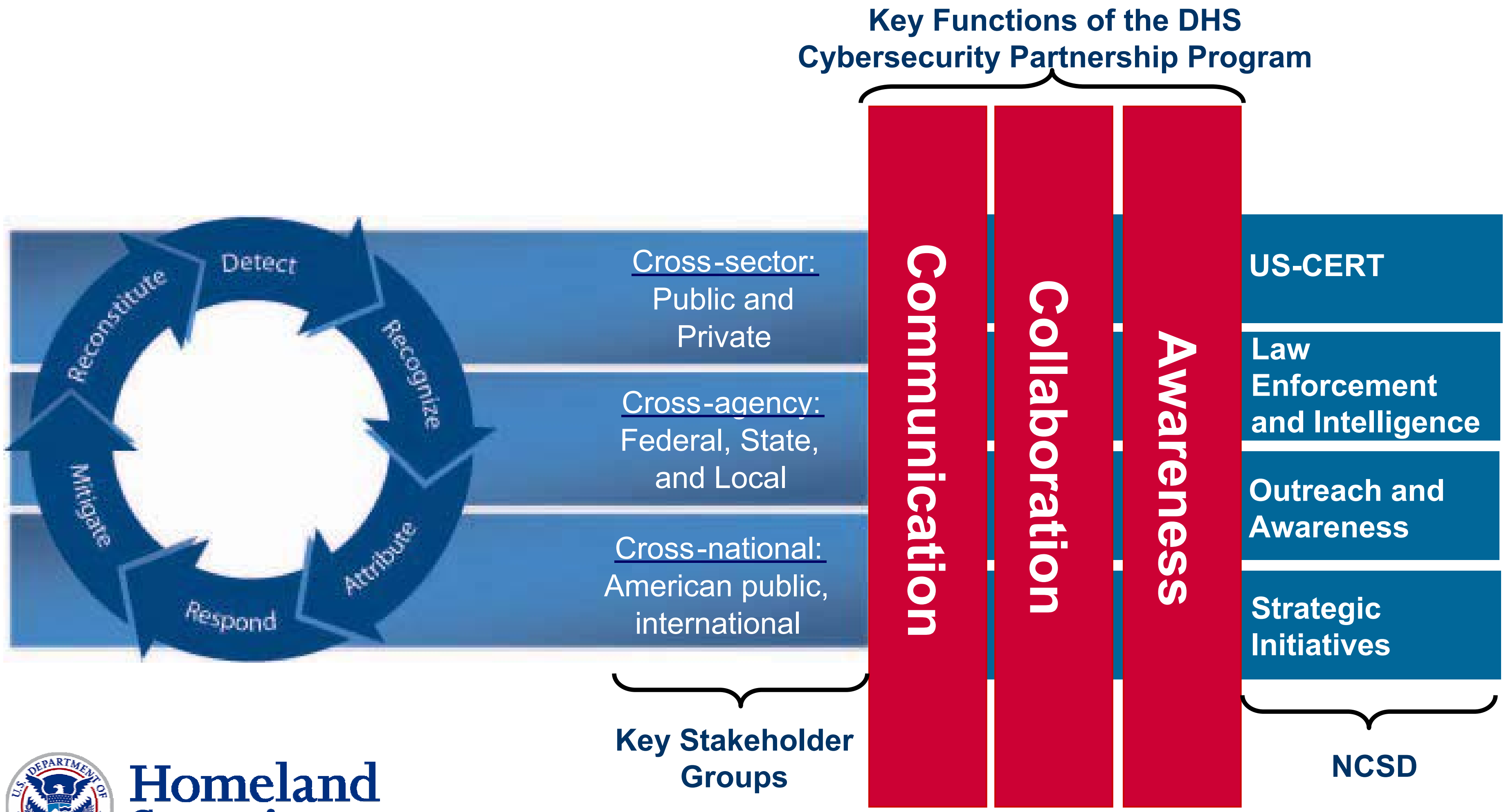
V. International Cyberspace Security Cooperation

HSPD-7: "…maintain an organization to serve as a focal point for the security of cyberspace.."

NCSD GOALS

1. Establish a National Cyber Security Response System to prevent, predict, detect, respond to, and reconstitute rapidly after cyber incidents.
2. Work with public and private sectors to reduce vulnerabilities and minimize the severity of cyber attacks.
3. Promote a comprehensive national awareness program to empower all Americans – businesses, the general workforce, and the general population – to secure their own parts of cyberspace.
4. Foster adequate training and education programs to support the Nation's cyber security needs.
5. Coordinate with the intelligence and law enforcement communities to identify and reduce threats to cyberspace.
6. Build a world-class organization that aggressively advances its cyber security mission and goals in partnership with its public and private stakeholders.

NCSD provides the framework for addressing cyber security challenges & Software Assurance needs



Key Functions of the DHS Cybersecurity Partnership Program

Cross-sector: Public and Private

Cross-agency: Federal, State, and Local

Cross-national: American public, international

Key Stakeholder Groups

Communication

Collaboration

Awareness

US-CERT

Law Enforcement and Intelligence

Outreach and Awareness

Strategic Initiatives

NCSD

Homeland Security