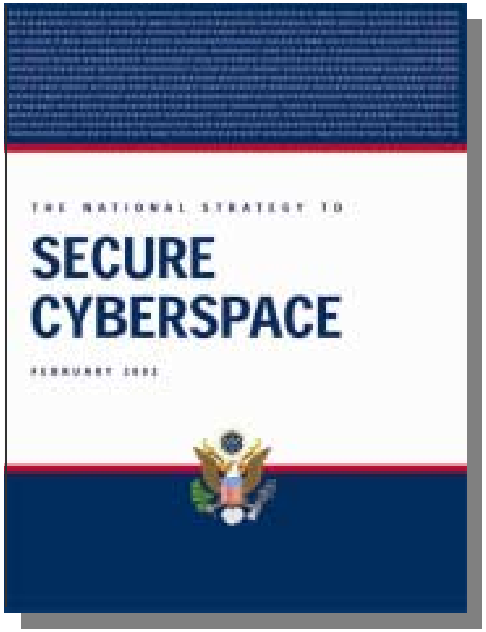
Software Assurance:

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 Modernization in Advancing a National Strategy to Secure Cyberspace

October 27 , 2005

Homeland Security

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

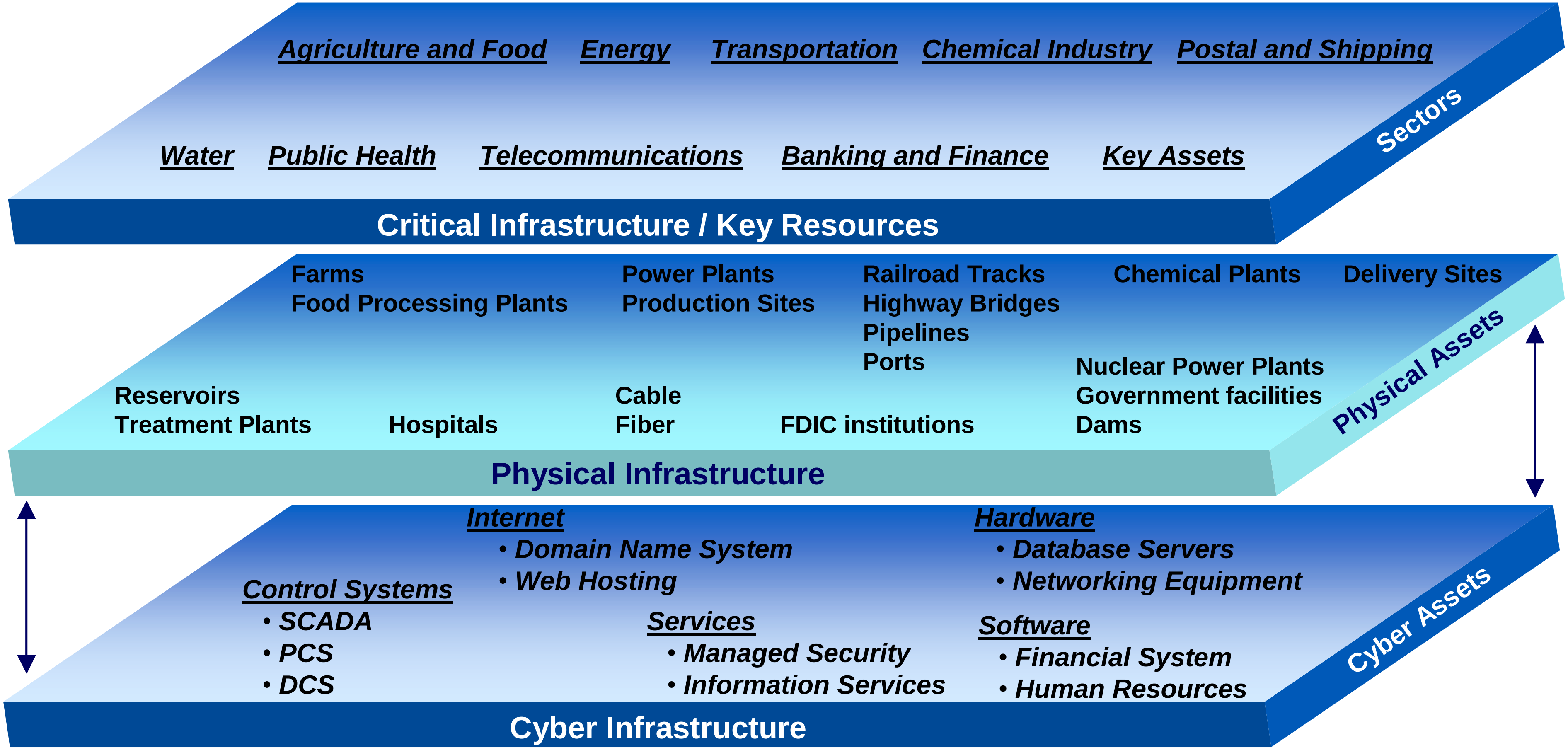
- Telecomm
  - 2B miles of cable
- Energy
  - 2,800 power plants
  - 300K production sites

- 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

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



Sectors

Agriculture and Food *Energy* *Transportation* *Chemical Industry* *Postal and Shipping*

Water *Public Health* *Telecommunications* *Banking and Finance* *Key Assets*

Critical Infrastructure / Key Resources

Physical Assets

Farms
Food Processing Plants

Power Plants
Production Sites

Railroad Tracks
Highway Bridges
Pipelines
Ports

Chemical Plants

Delivery Sites

Nuclear Power Plants
Government facilities
Dams

Reservoirs
Treatment Plants

Hospitals

Cable
Fiber

FDIC institutions

Physical Infrastructure

Cyber Assets

Control Systems
- *SCADA*
- *PCS*
- *DCS*

Internet
- *Domain Name System*
- *Web Hosting*

Services
- *Managed Security*
- *Information Services*

Hardware
- *Database Servers*
- *Networking Equipment*

Software
- *Financial System*
- *Human Resources*

Cyber Infrastructure

Homeland Security

Need for secure software applications

National Cyber Security Division (NCSD) goals are strategically aligned to four frameworks

Mandates	
National Strategy to Secure Cyberspace	I. National Cyberspace Security Response System
	II. National Cyberspace Threat and Vulnerability Reduction Program
	III. Nation 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.."
NIPP	Provides a consistent, unifying structure for integrating the current multitude of CIP efforts into a single national program
NRP "Cyber Annex"	Describes framework for Federal cyber incident response coordination among Federal departments and agencies

NCSD GOALS

1. Establish a National Cyber Security Response System to prevent, 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.

National Strategy to Secure Cyberspace

- Outlines a framework for organizing and prioritizing efforts
- Provides direction to federal government departments and agencies
- Identifies steps to improve our collective cyber security
- Highlights role of public-private engagement
- Outlines Strategic Objectives

1	2	3
Prevent cyber attacks against America's critical infrastructures	Reduce national vulnerability to cyber attacks	Minimize damage and recovery time from cyber attacks that do occur

Homeland Security

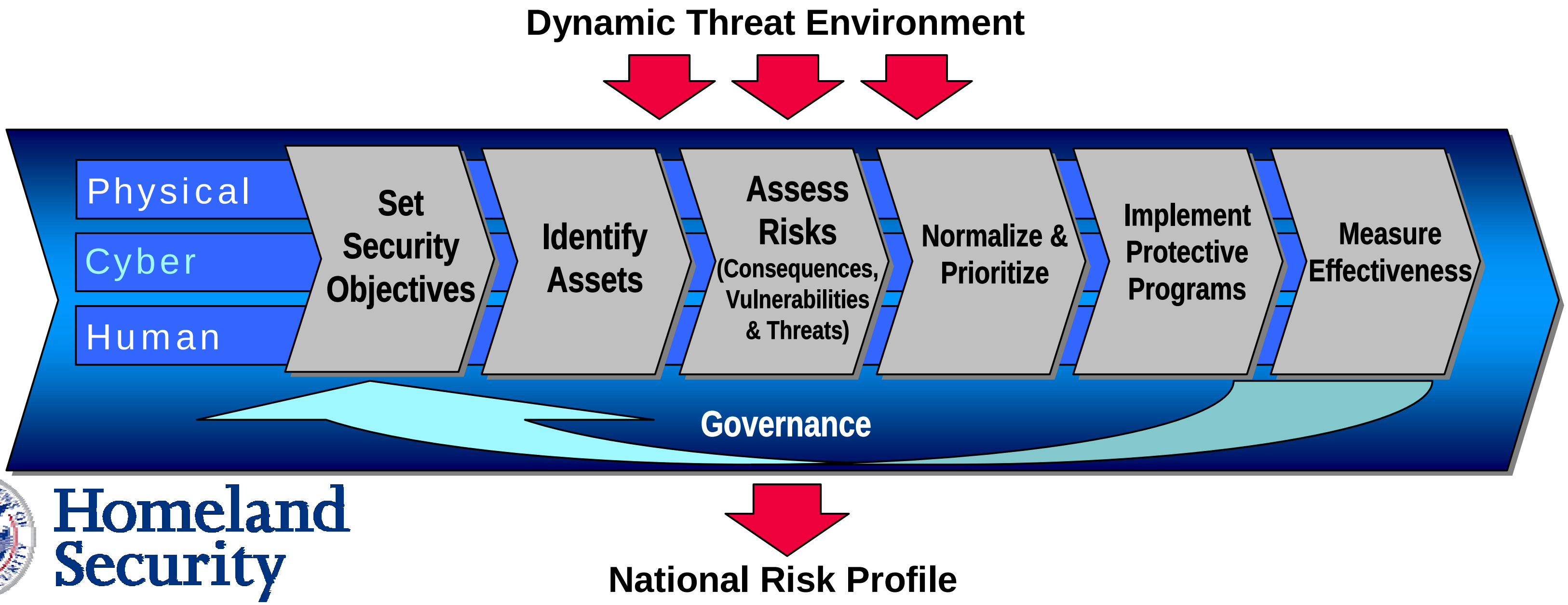
HSPD-7: A national policy to protect our nation's infrastructure

- Maintain an organization to serve as a focal point for the security of cyberspace
- Facilitate interactions and collaborations between and among federal departments and agencies, state and local governments, the private sector, academia, and international organizations
- Execute a mission including analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical information systems

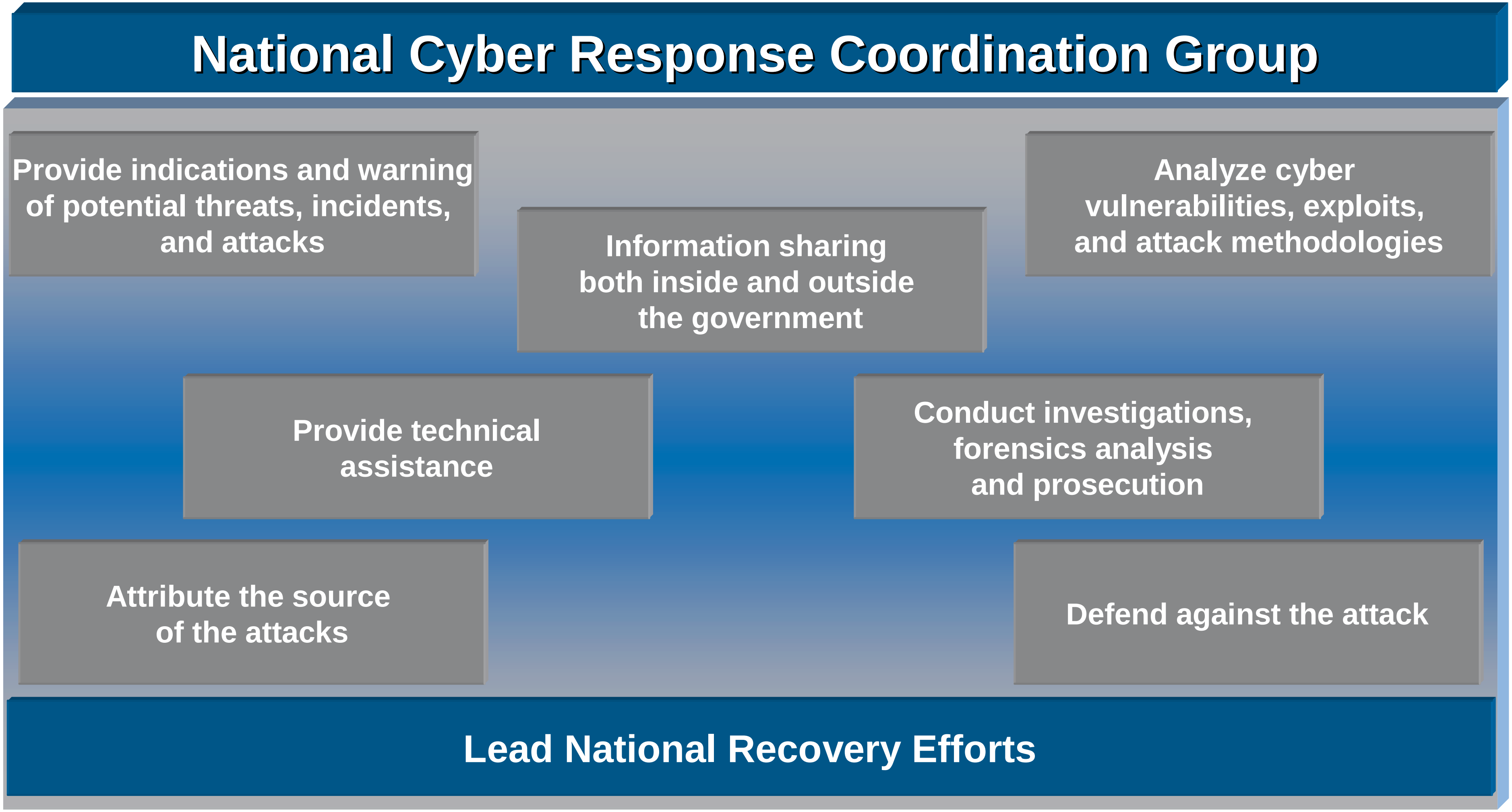
The NIPP outlines a unifying structure

- 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 (IT) sector

NIPP Risk Management Framework



NRP Cyber Annex describes the framework for response coordination



National Cyber Response Coordination Group

Provide indications and warning of potential threats, incidents, and attacks

Information sharing both inside and outside the government

Analyze cyber vulnerabilities, exploits, and attack methodologies

Provide technical assistance

Conduct investigations, forensics analysis and prosecution

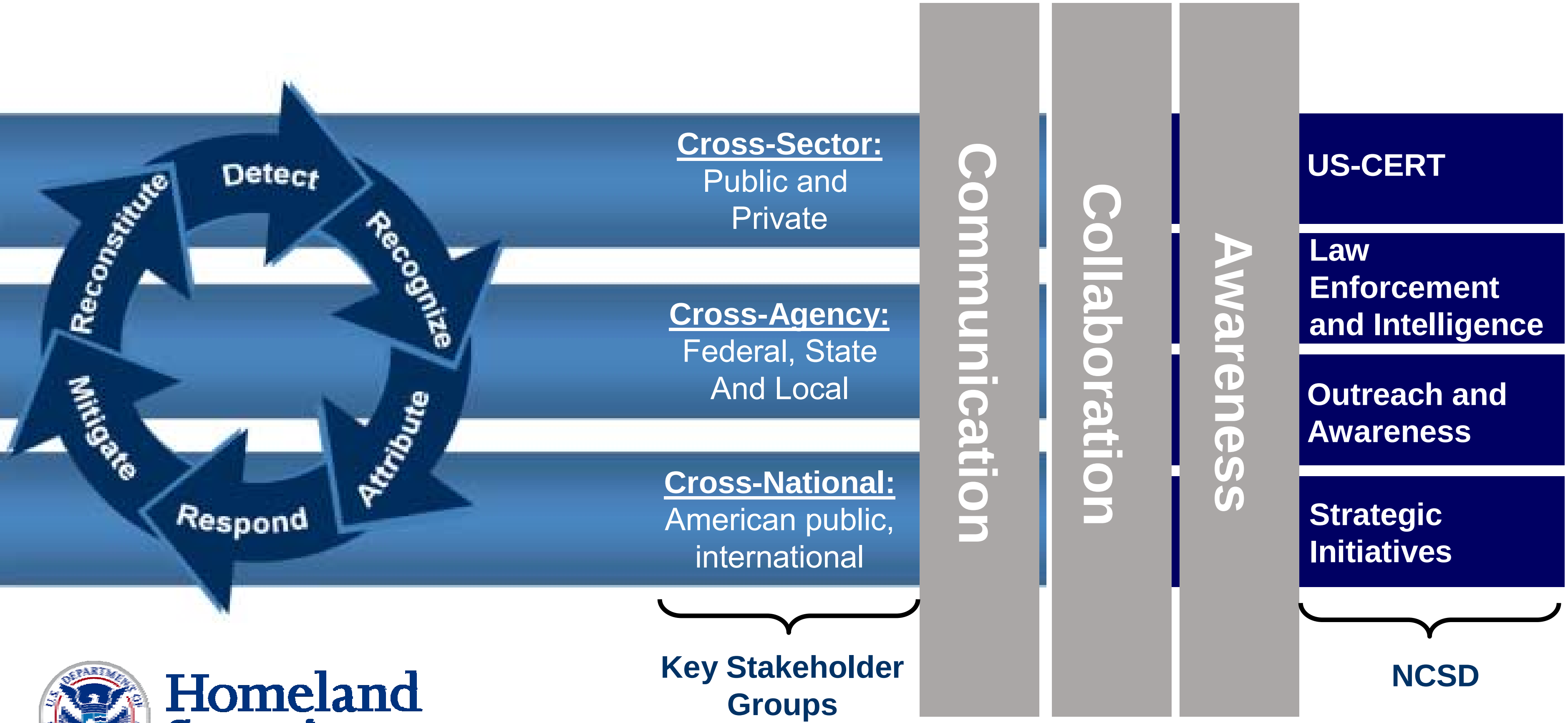
Attribute the source of the attacks

Defend against the attack

Lead National Recovery Efforts

DHS National Cyber Security Division (NCSD) provides the framework for addressing cyber security and software assurance challenges

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

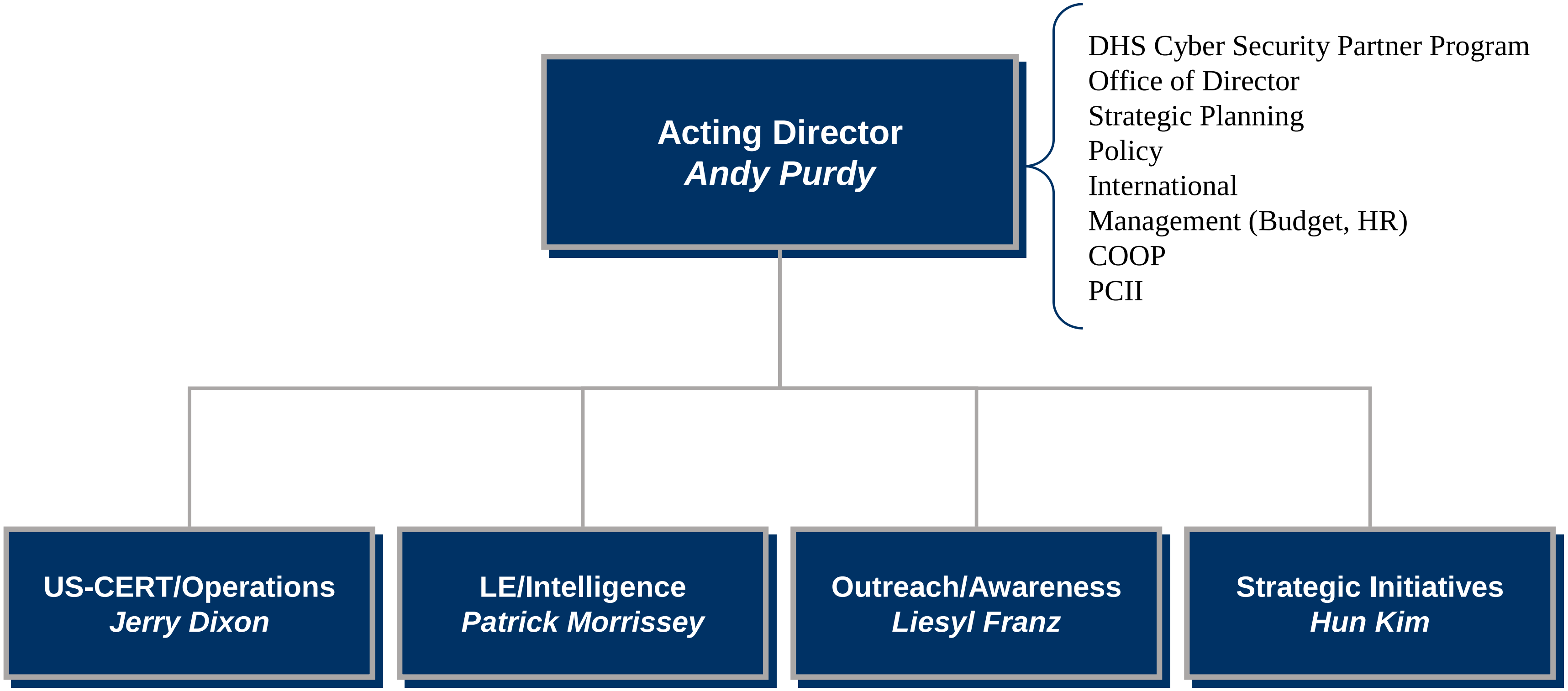
Law Enforcement and Intelligence

Outreach and Awareness

Strategic Initiatives

NCSD

DHS National Cyber Security Division



Acting Director
Andy Purdy

DHS Cyber Security Partner Program
Office of Director
Strategic Planning
Policy
International
Management (Budget, HR)
COOP
PCII

US-CERT/Operations
Jerry Dixon

Situational Awareness
Analytical Cell
Production
Federal Coordination

LE/Intelligence
Patrick Morrissey

Intel Requirements
LE Coordination
NCRCG

Outreach/Awareness
Liesyl Franz

Communications
Messaging
Outreach to Stakeholders
Cyber Security Awareness
Partnerships

Strategic Initiatives
Hun Kim

CIP Cyber Security
Control Systems Security
Software Assurance
Training & Education
Exercise Planning & Coordination
Standards & Best Practices
R&D Coordination

Driving Needs for Software Assurance

- Software vulnerabilities jeopardize: infrastructure operations, web-based applications & services, business operations & services, intellectual property, 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 lifecycle processes offer opportunities to insert malicious code and to poorly design and build software which enables future 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

Homeland Security

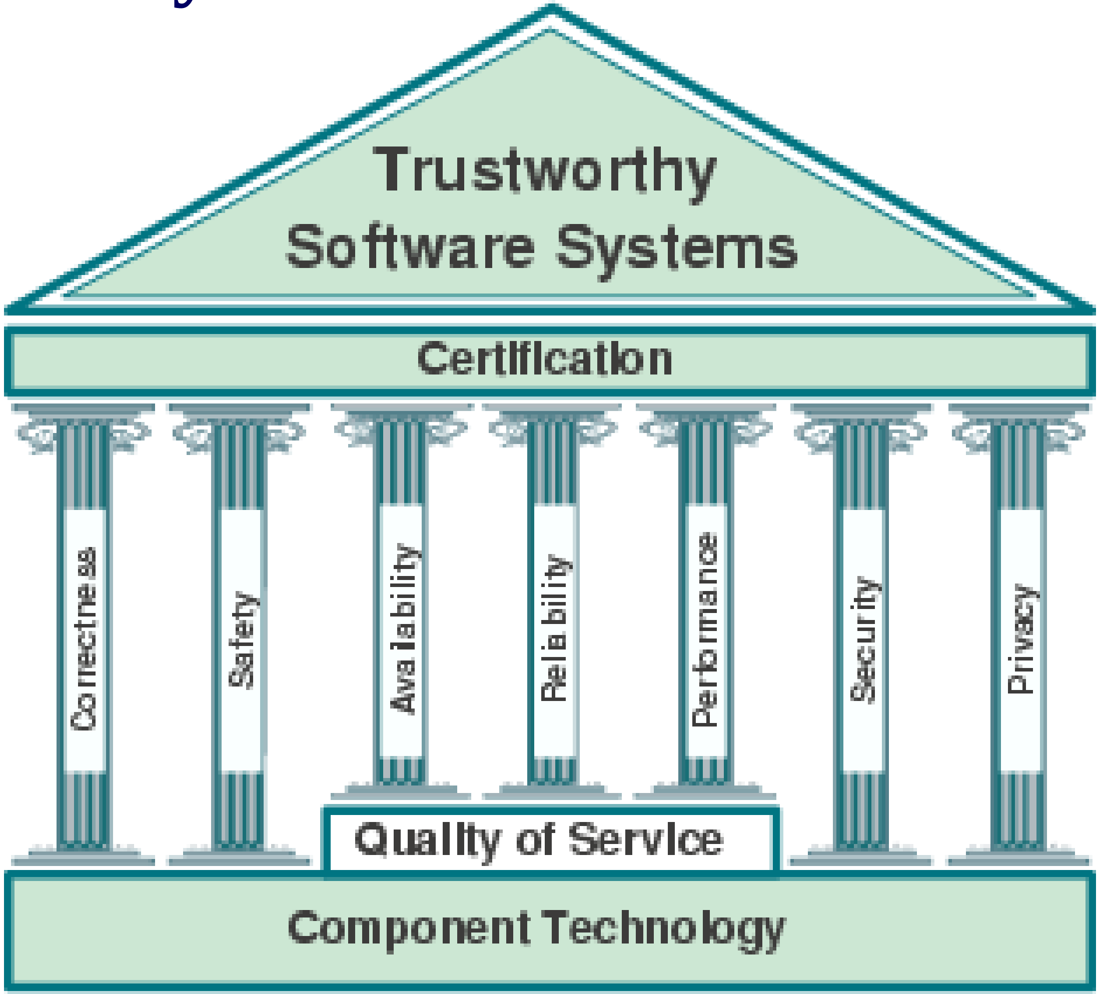
Strengthen operational resiliency

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

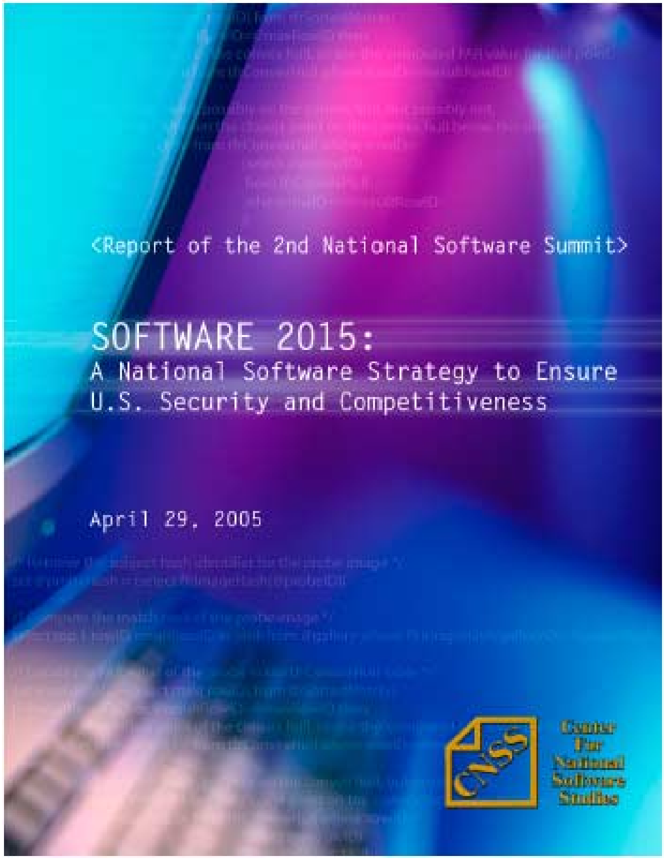


Adopted from the TrustSoft Graduate School on Trustworthy Software Systems, started April 2005; funded by the German Research Foundation (DFG). See German Oldenburg http://trustsoft.uni-oldenburg.de

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

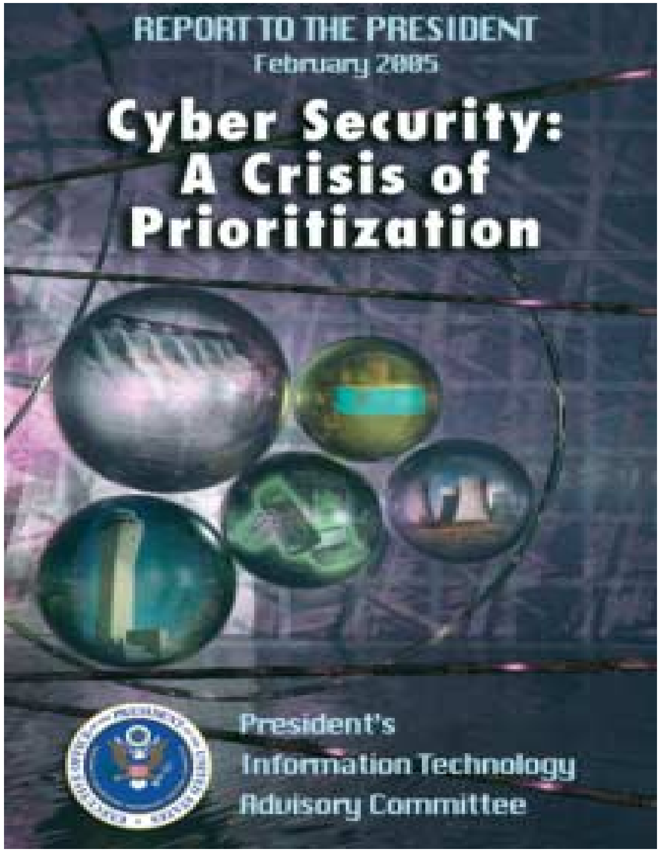
*** See report at Center for National Software Studies www.cnsoftware.org/nss2report**

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' [Note: PITAC is now a part of PCAST]

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
- GAO R&D study on “risks attributable to outsourcing of software throughout critical infrastructure” being completed

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

What has Caused Software Assurance Problem

Increasing software vulnerabilities and exploitation

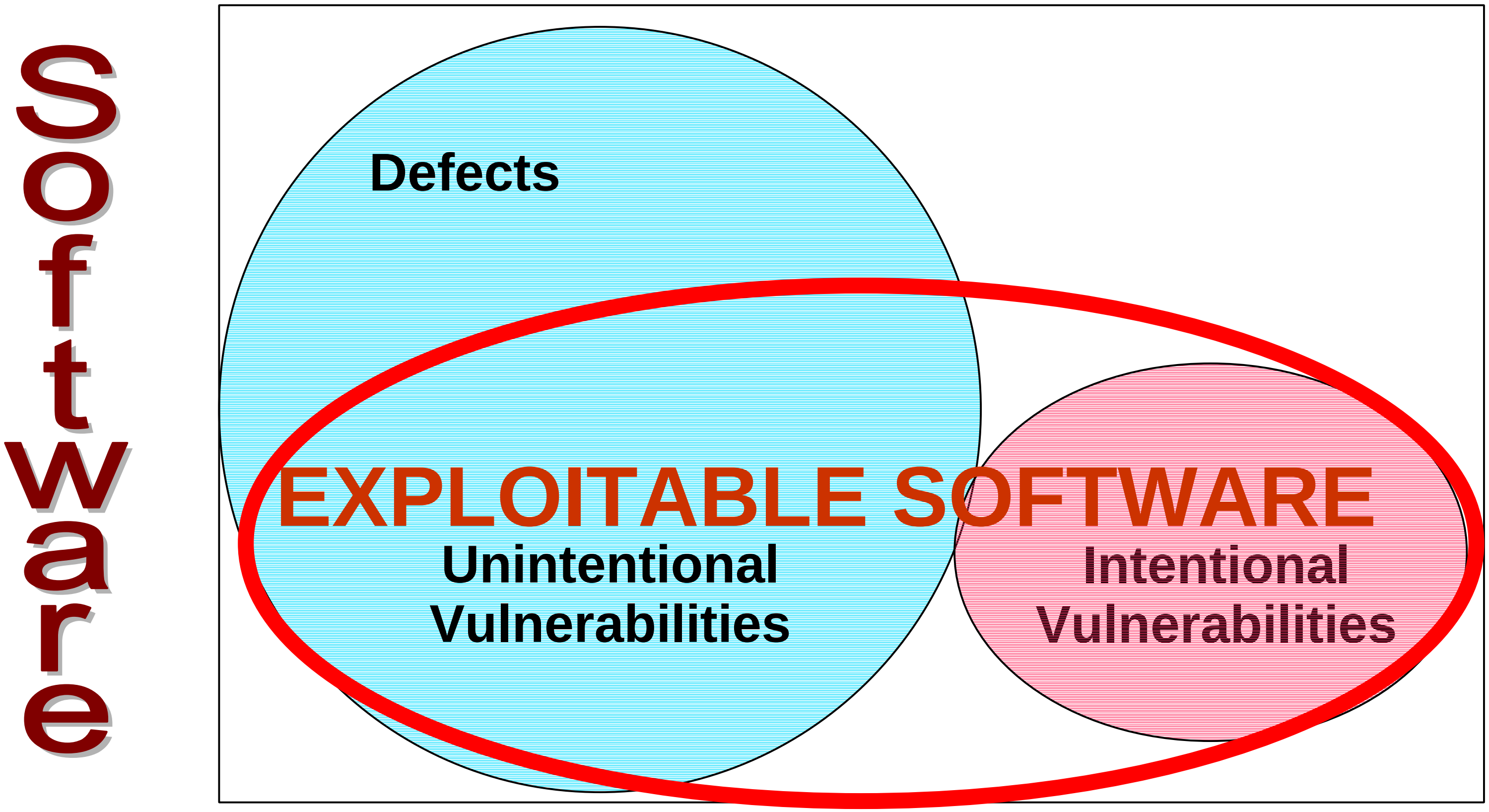
- Then
  - Domestic dominated market
  - Stand alone systems
  - Software small and simple
  - Software small part of functionality
  - Custom and closed development processes (cleared personnel)
  - Adversaries known, few, and technologically less sophisticated

- 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

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

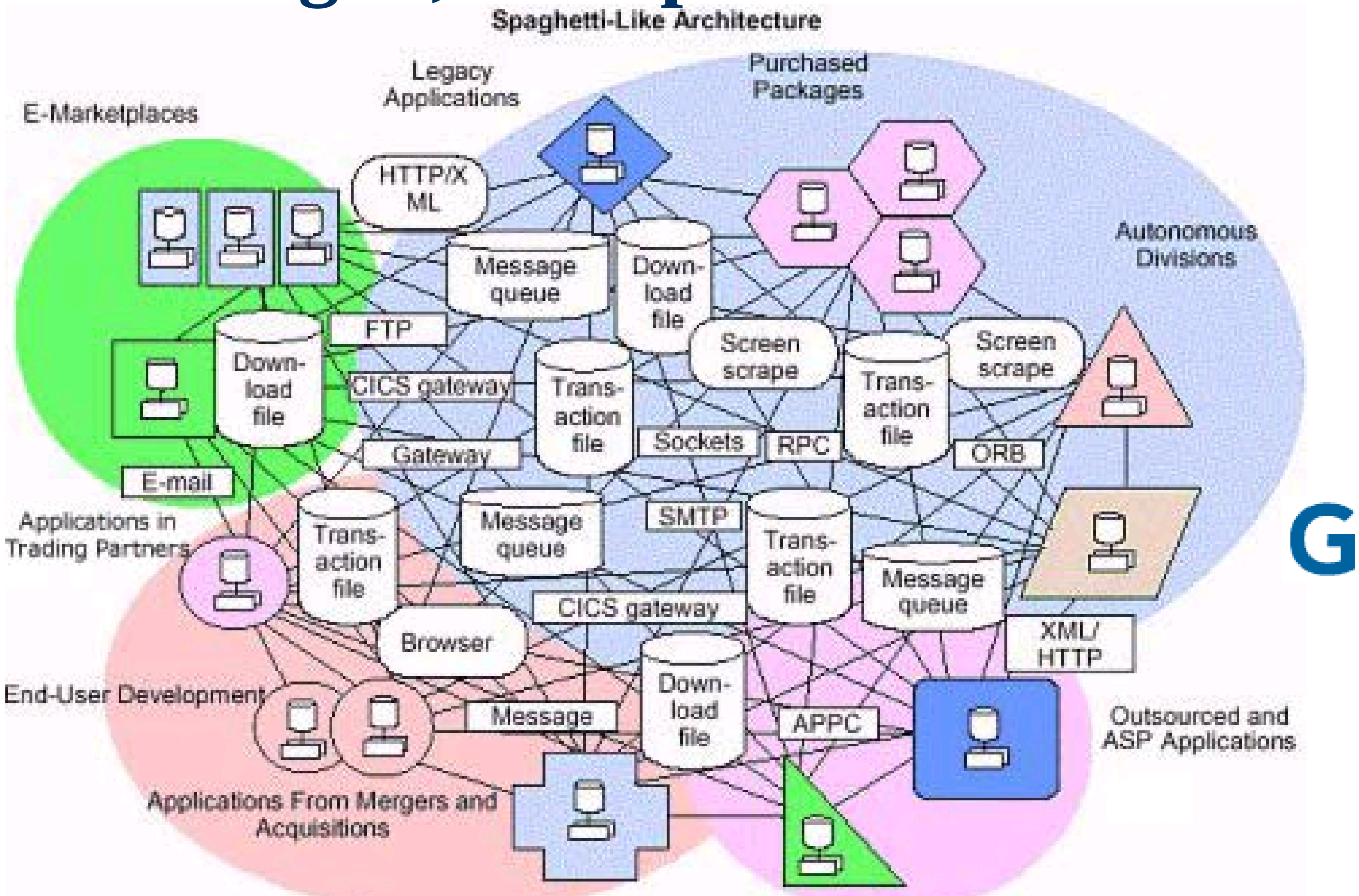
Realities of Relying on Software

- Software has defects – many defects have security implications.
- As new attacks are being invented, software behaviour that could reasonably have been considered correct when written may have unintended effects when deliberately exploited.
- Current software patching solutions are struggling to catch up with the attacks.
- Since hackers are trying to break into system at every level of the application stack, heap or registry, it’s critical to understand the security implications of programming decisions in order to keep your software secure.

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

Reality of Existing Software: complex, multiple technologies, multiple vendors

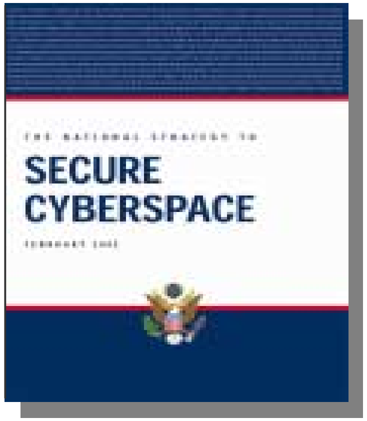


Gartner

- 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

DHS Software Assurance Program Overview



THE NATIONAL STRATEGY TO

SECURE CYBERSPACE

FEBRUARY 2003

- 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 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 Comes From:

Knowing what it takes to "get" what we want

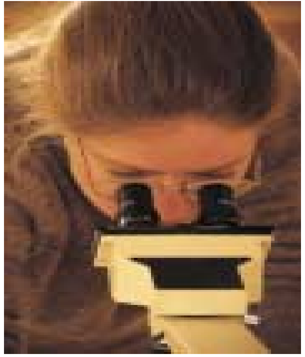
- Development/acquisition practices/process capabilities
- Criteria for assuring integrity & mitigating risks

Building and/or acquiring what we want

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

*Multiple Sources:

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



Understanding what we built / acquired

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

Using what we understand

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

Homeland Security

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

Software Assurance Program Alignment

	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

Homeland Security

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

Software Assurance Program Alignment – FY05

	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 – Draft Build Security In Web site – launched 3 Oct	SwA Common Body of Knowledge – Draft 0.7 Articles in journals SwA Forums, workshops and conferences	Tools and Product Evaluation NIAP Review SEMATE: Metrics and Tool Evaluation	Processes and Practices National & International standards SwA security measurement	Software Assurance Program Management – SwA Director hired 21 Mar 2005

Homeland Security

Software Assurance Program Alignment – FY06

	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 – final March 2006 Build Security In Web site – stakeholder review, CCB, updates	SwA Common Body of Knowledge – version 1.0 in March 2006 Articles in journals SwA Forums, workshops and conferences	Federated Labs - Tools and Product Evaluation (NIAP Review) SEMATE: Metrics and Tool Evaluation Acquisition Guides: Procurement templates	Processes and Practices National & International standards SwA security measurement	Software Assurance Program Management – SwA Deputy Director/ Program Mgr to be hired (already selected)

Homeland Security

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

DHS SwA Program Alignment with Related Initiatives – National Software Strategy

- ►DHS SW Assurance Program
  - People – developers (includes education and training) and users
  - Processes – best practices, standards, and practical guidelines for development of secure software
  - Technology – evaluation tools and cyber security R&D
  - Acquisition – software security improvements in specifications and guidelines for acquisition and outsourcing

- NSG Software Strategy
  - Improving SW Trustworthiness
    - Trustworthy SW Measurement & Analysis
    - Trustworthy SW Development
    - Trustworthy SW Ed & Awareness
    - Trustworthy SW Business Practices
    - Trustworthy SW R&D
  - Educating & Fielding SW Workforce
    - Science & Eng Revitalization
    - SW Engineering Education
    - Understanding Impact of Offshore Outsourcing on Workforce
  - Re-energizing SW R&D
    - SW R&D Roadmap (Grand Challenges & SW capability Business Case Development)
    - Government-led Strategic SW R&D
  - Encouraging Innovation in US SW industry
    - Software Innovation Initiative

DHS NCSD Director for Software Assurance is a member of the National Steering Group

DHS SwA Program Alignment with Related Initiatives – DoD SwA Initiative

►DHS SW Assurance Program

- People – developers (includes education and training) and users
- Processes – best practices, standards, and practical guidelines for development of secure software
- Technology – evaluation tools and cyber security R&D
- Acquisition – software security improvements in specifications and guidelines for acquisition and outsourcing

► DoD SwA Initiative - Tiger Team

- Engineering-in-Depth
  - SwA in Engineering Processes
  - SwA planning in Systems Engineering Plans
  - SwA planning in Test & Evaluation Plans
  - Industry standards and metrics
  - Enhancements in acquisition guidance
- Industry Outreach
  - Defense Trade Associations
  - Standards Organizations
- Science & Technology
  - Executive Agent for SW Vulnerability Mitigation and Discovery
  - Center for Assured Software with key partners

Homeland Security

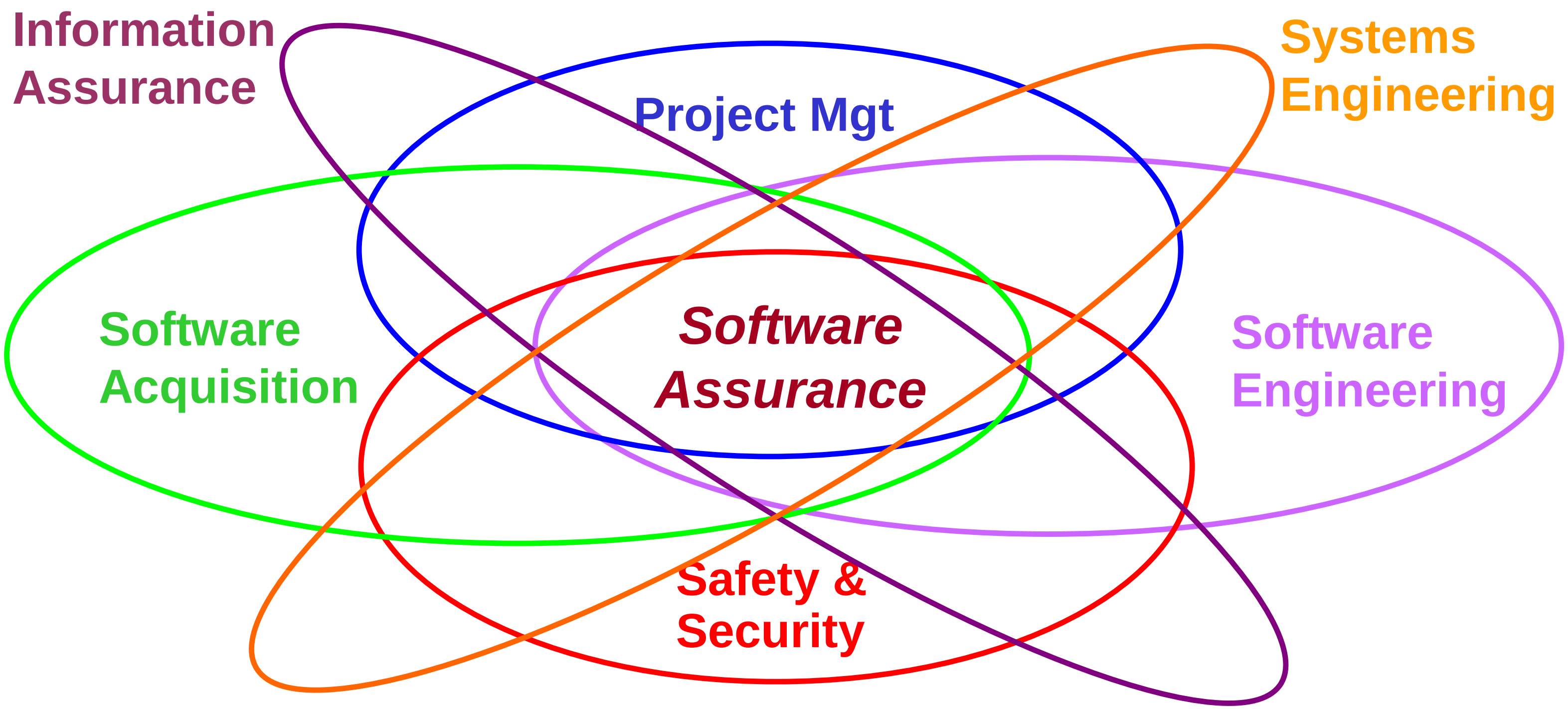
DHS NCSD collaborates with DoD via WGs, Standards Organizations and DoD SwA Executive Roundtable

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 Electronic Develop a Curriculum Event and CBK Working Groups (April, June, August, and October 2005) to develop CBK that involved participation from academia, industry and Federal Government
  - **Addressing three domains: “acquisition & supply,” “development,” and “post-release assurance” (sustainment)**
  - **Distributed CBK v0.7 in October 2005**, with v.0.9 in January 2006 and v1.0 by March 2006
  - Developed CBK awareness materials, including Frequently Asked Questions by Oct 2005 with update in January 2006
  - Develop 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:

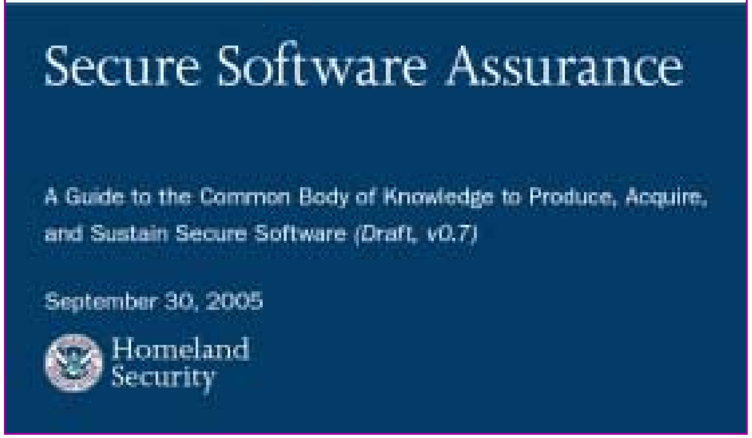
- A “knowledge area” extension within each of the contributing disciplines;
- A stand-alone CBK drawing upon contributing disciplines;
- A set of functional roles, drawing upon a common body of knowledge; allowing more in-depth coverage dependent upon the specific roles.

Secure Software Assurance

A Guide to the Common Body of Knowledge to Produce, Acquire and Sustain Secure Software, v0.7

- Further review and comments have been solicited for feedback by November 15, 2005 -- broader stakeholder community being contacted
- To provide comments, people must join 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 to be released in Jan 2006 via Federal Registry, with v1.0 to be published by March 2006**
- Offered for informative use; it is not intended as a policy or a standard

Information for Educators & Trainers



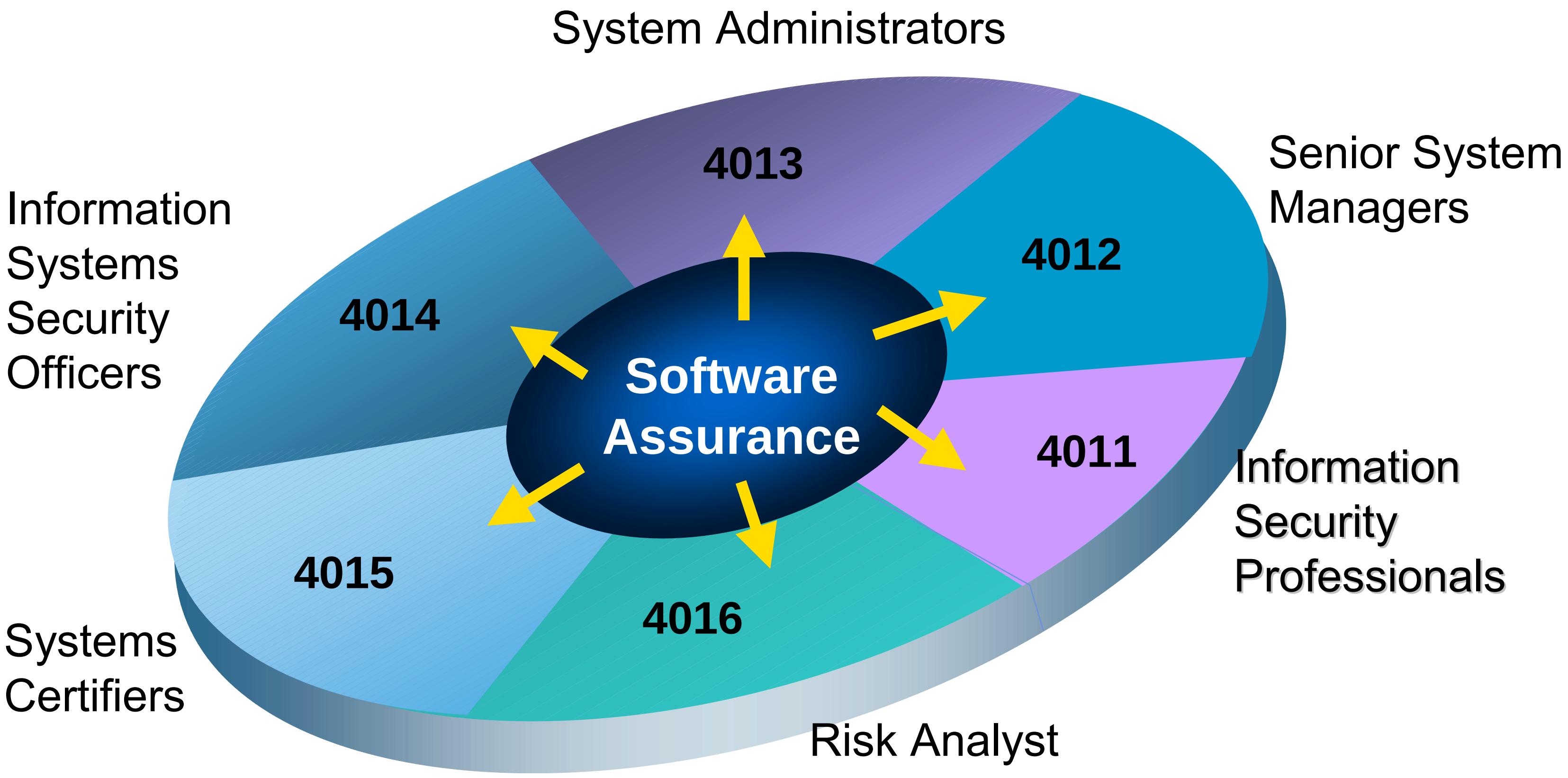
Secure Software Assurance

A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software *(Draft, v0.7)*

September 30, 2005

Homeland Security

Integrating SwA CBK with CNSS IA Standards



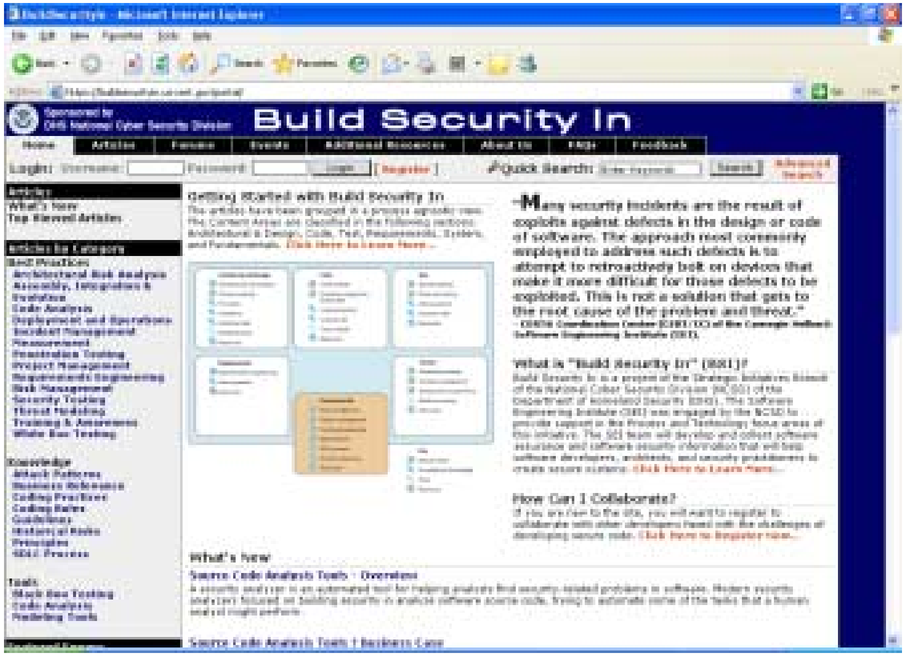
Software Assurance considerations for IA functional roles:

-- add SwA material in each CNSS 4000 series standard

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

Software Assurance: Process

- 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 “**buildsecurityin.us-cert.gov** on October 3, 2005
    - – Provides dissemination of recommended 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



Getting Started with Build Security In

“Many security incidents are the result of exploits against defects in the design or code of software. The approach most commonly employed to address such defects is to attempt to retroactively bolt on devices that make it more difficult for those defects to be exploited. This is not a solution that gets to the root cause of the problem and threat.”

What is “Build Security In” (BSI)?

How Can I Collaborate?

What's New

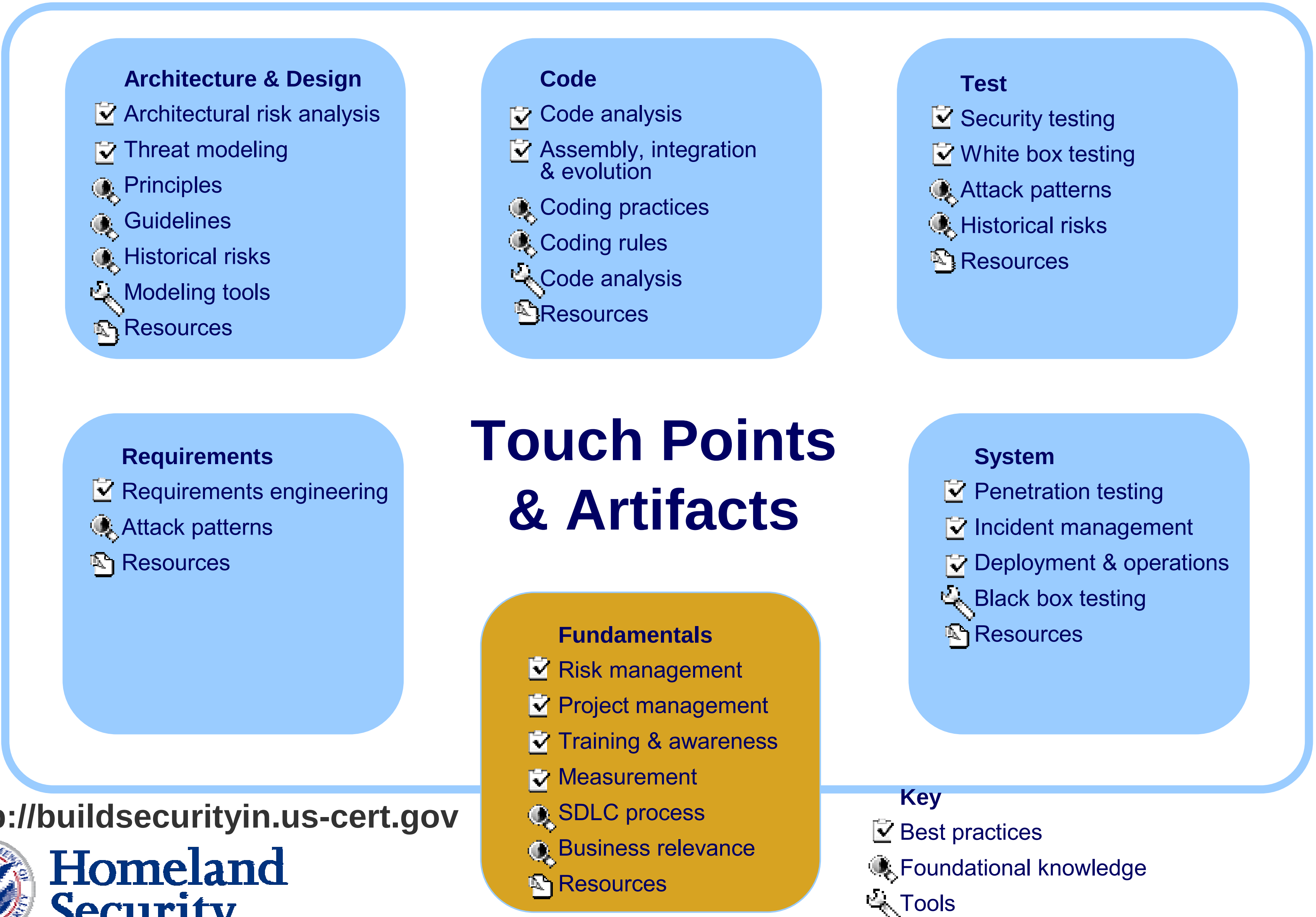
Source Code Analysis Tools - Overview

Source Code Analysis Tools : Business Case

**NCSD Goal Action 2.3.2

Process Agnostic Lifecycle

Launched 3 Oct 2005



Touch Points & Artifacts

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

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 practices
- 🔍 Foundational knowledge
- 🔧 Tools
- 📄 Resources

http://buildsecurityin.us-cert.gov

Homeland Security

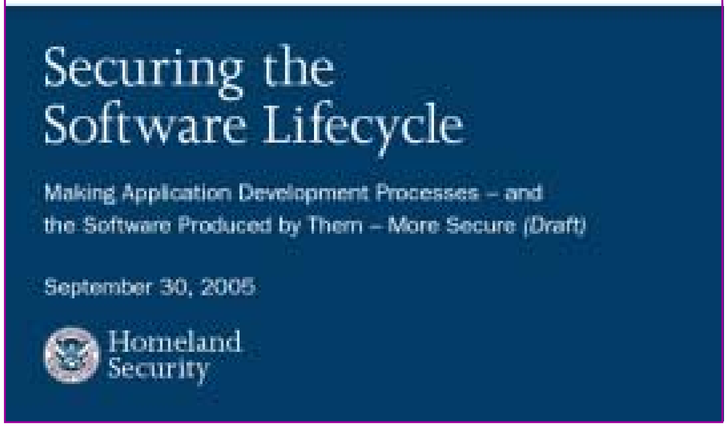
Software Assurance: Process (cont.)

- Provide practical guidance in software assurance practices and process improvement methodologies** (cont.)
  - Released draft developers' guide "SECURING THE SOFTWARE LIFECYCLE: Making Application Development Processes – and Software Produced by Them – More Secure"

- Collect, develop, and publish practical guidance and reference materials for security through the software development life cycle

- Provide an informative aid for developers on software assurance process improvement methodologies.

Information for Developers



Securing the Software Lifecycle

Making Application Development Processes – and the Software Produced by Them – More Secure *(Draft)*

September 30, 2005

Homeland Security

“Securing the Software Lifecycle:
Making Application Development Processes – and the Software Produced by Them – More Secure” (draft)

- 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

Securing the Software Lifecycle

Making Application Development Processes – and the Software Produced by Them – More Secure (Draft)

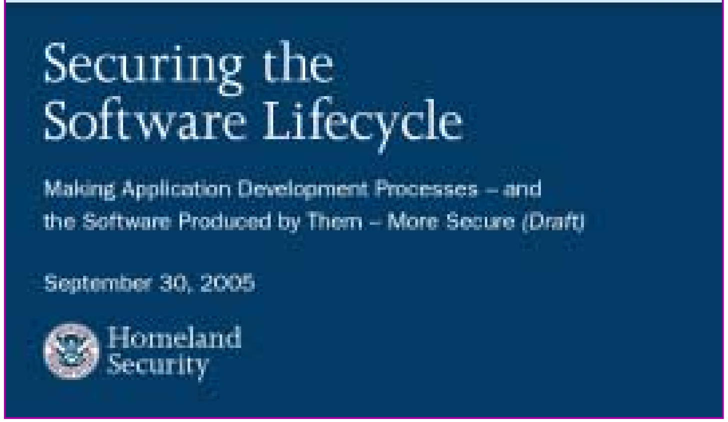
September 30, 2005

Homeland Security

“Securing the Software Lifecycle:
Making Application Development Processes – and the Software Produced by Them – More Secure” (draft)

- Offered for informative use; it is not intended as a policy or standard
  - Further review and comments have been solicited for feedback by November 15, 2005 -- broader stakeholder community being contacted
  - To provide comments, people must join Software Processes and Practices WG to collaborate through the US CERT Portal (https://us-cert.esportals.net/) using Organization ID 223
- Next draft version to be released in Jan 2006 via Federal Registry, with v1.0 to be published by March 2006

Information for Developers



Securing the Software Lifecycle

Making Application Development Processes – and the Software Produced by Them – More Secure (Draft)

September 30, 2005

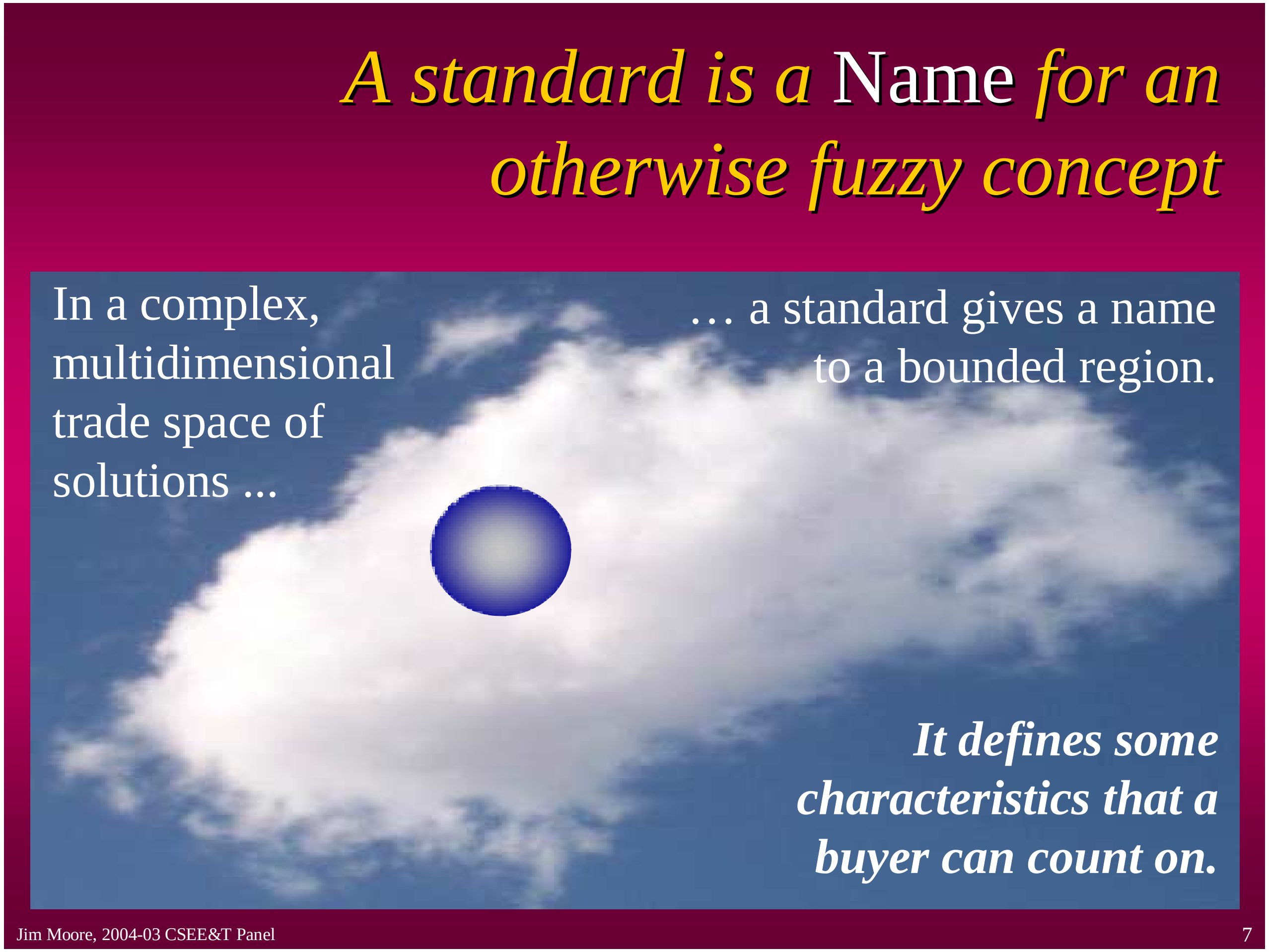
Homeland Security

Software Assurance: Process (cont.)

- Provide practical guidance in software assurance process improvement methodologies** (cont.)
  - 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)
  - Continue 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 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

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

Role of Standardization for Software Assurance

- SwA standards are needed to better enable exchange of information between participants and enable interoperability between solutions (provided by multiple vendors) needed to perform SwA activities.
  - SwA Standards should allow different participants to initiate collaboration and activities in area of SwA through the common framework and achieve greater automation of SwA processes by enabling interoperability between different supporting tools
- Standardization would increase interoperability among tools and manual processes by creating an open framework.
- Standardization would enable a new generation of solutions to benefit all sectors (Government, Industry and others)
- Standardization would ensure that all sectors are investing within the context of a coordinated strategy.

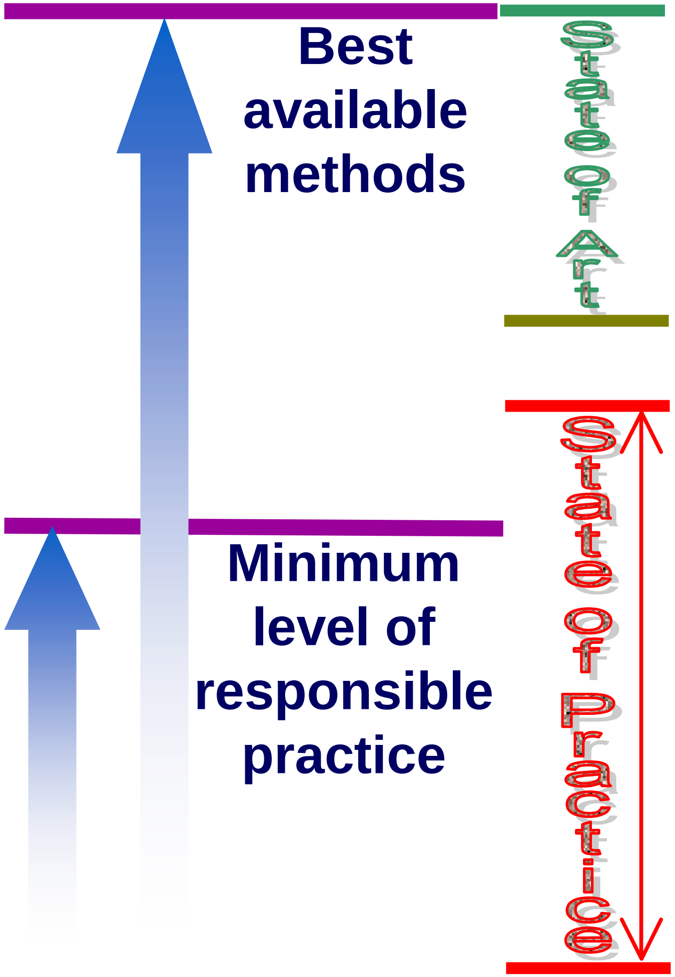
Using Standards and Best Practices to Close gaps between state-of-the-practice and state-of-the-art *[1, 2]

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."



Best available methods

State of Art

Minimum level of responsible practice

State of Practice

*[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

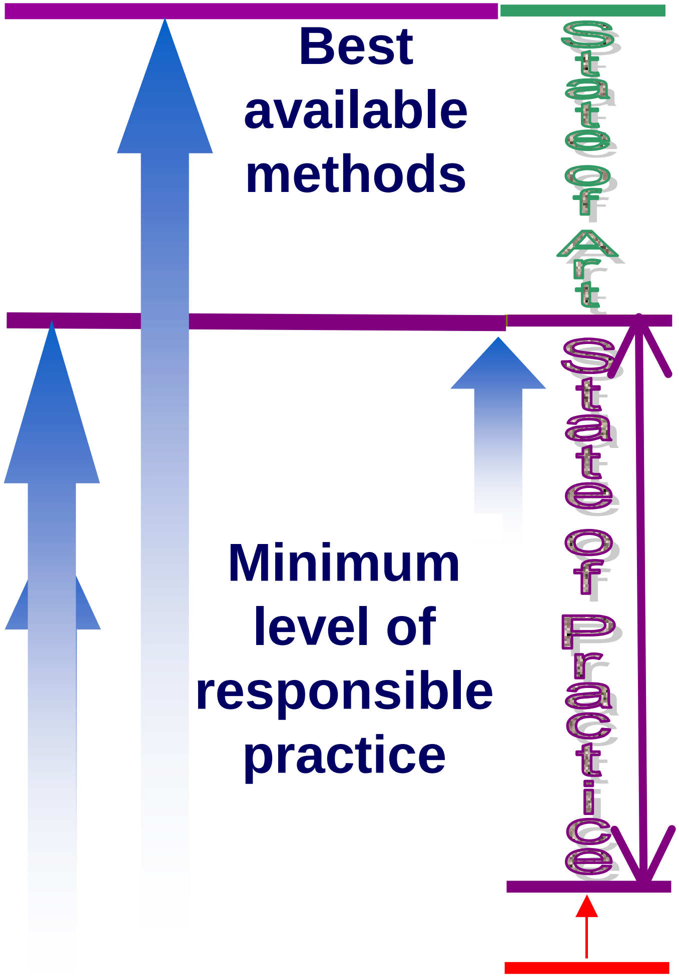
Using Standards and Best Practices to Close gaps between state-of-the-practice and state-of-the-art *1, 2

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.

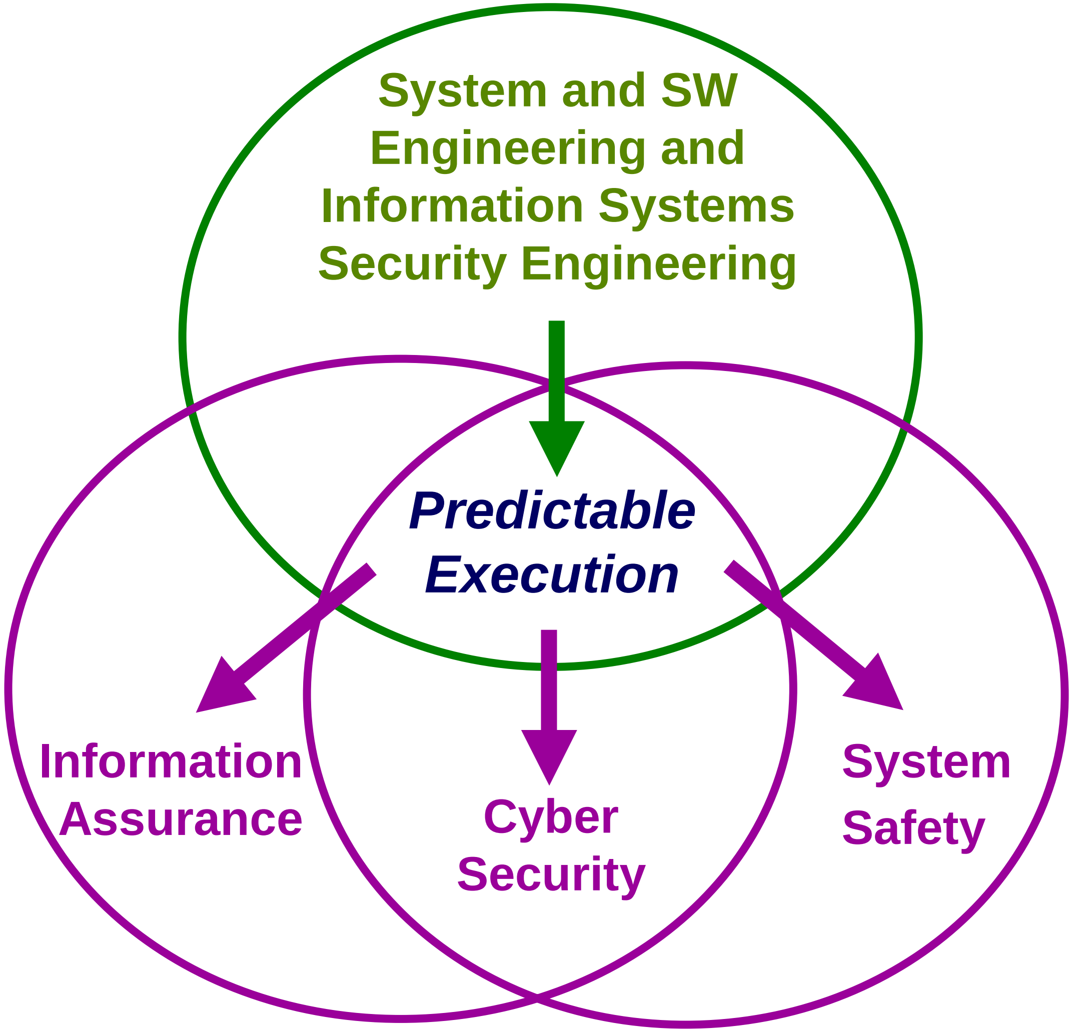
Raising the Floor

- 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 …

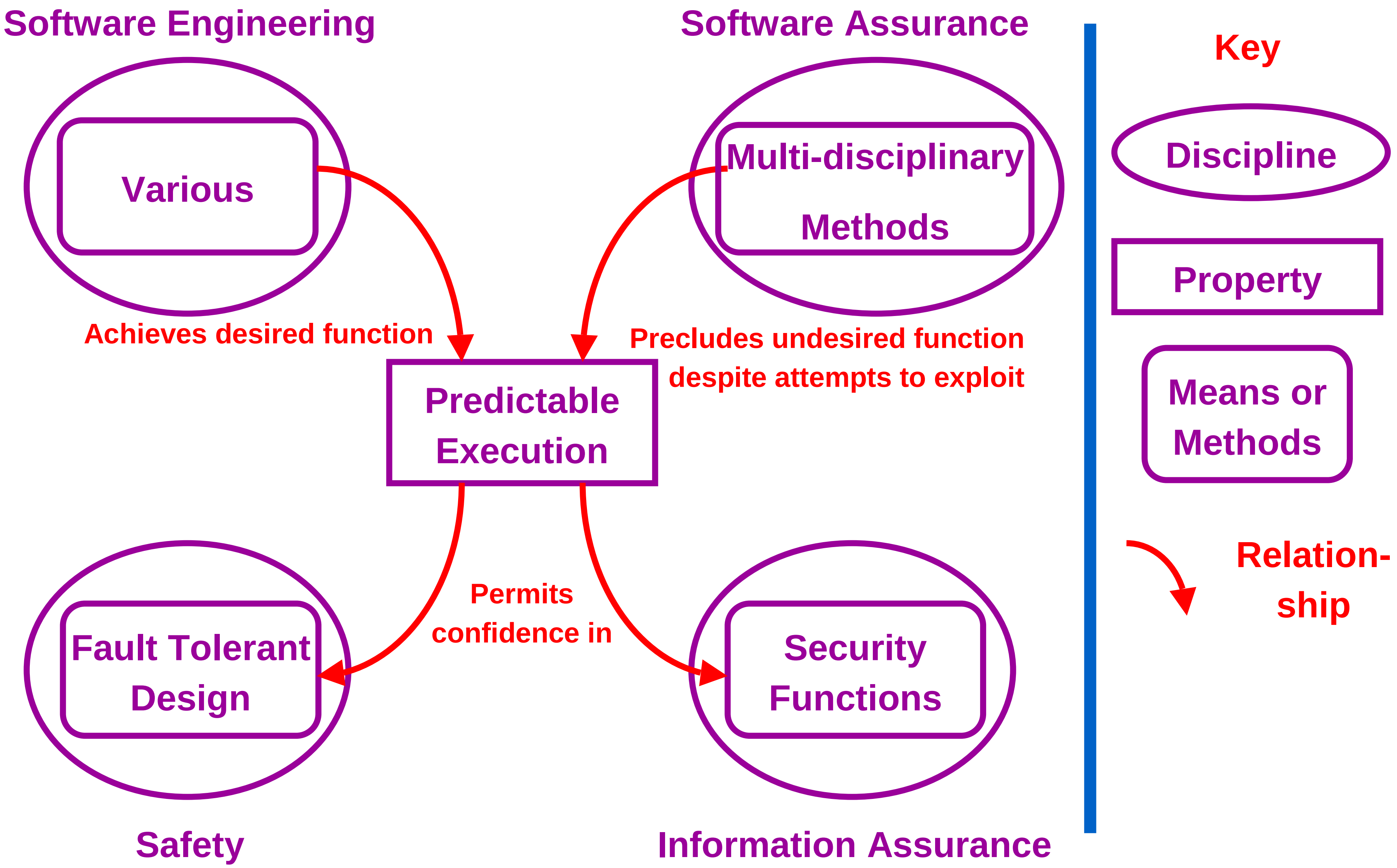
- Correct implementation of requirements, expectations and regulations.
- Exclusion of unwanted function even in the face of attempted exploitation.

Traditional concern

Growing concern

Homeland Security

Simplified Relationships among Disciplines



Software Engineering

Various

Achieves desired function

Software Assurance

Multi-disciplinary Methods

Precludes undesired function despite attempts to exploit

Predictable Execution

Permits confidence in

Fault Tolerant Design

Safety

Security Functions

Information Assurance

Key

Discipline

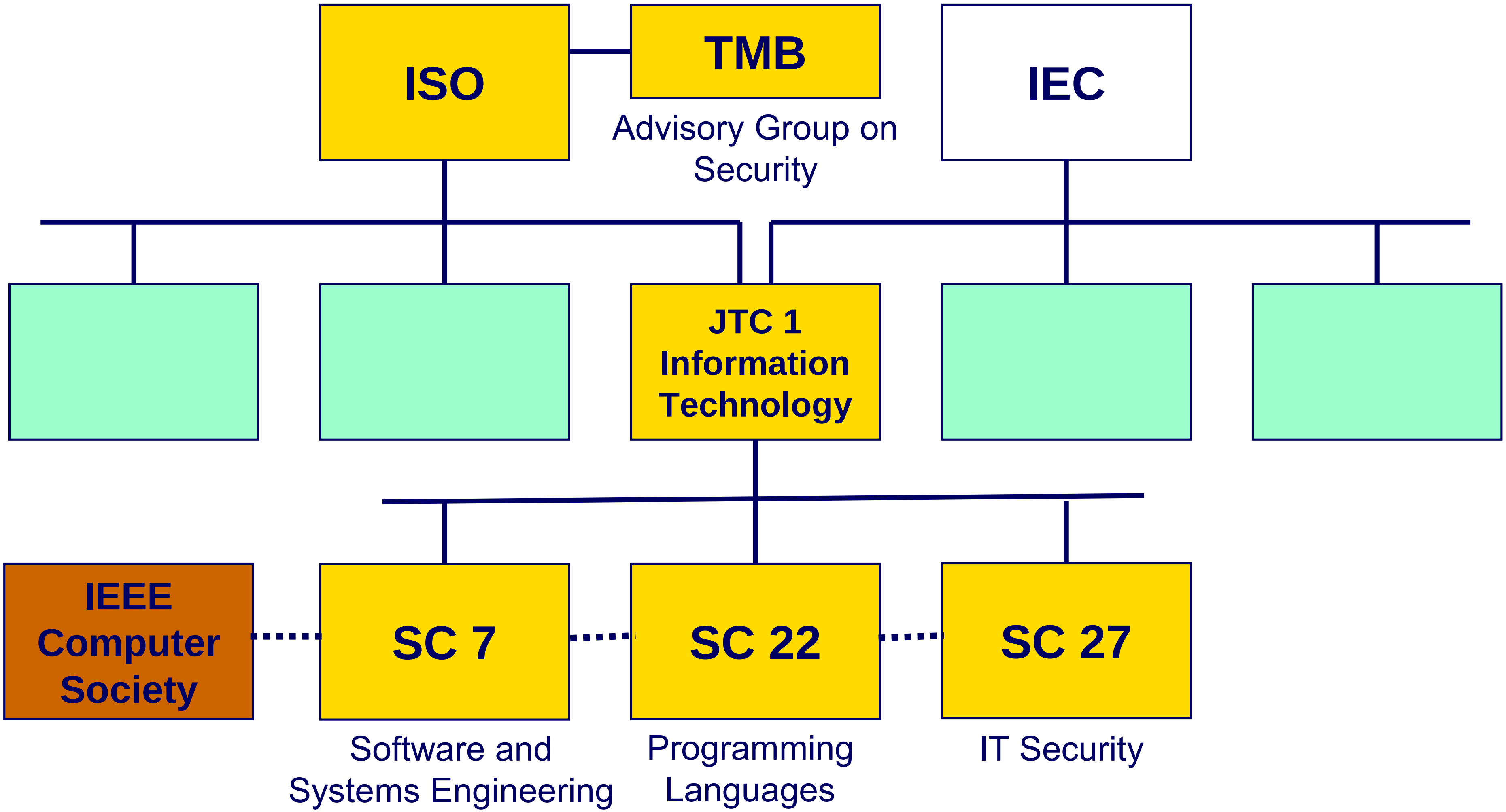
Property

Means or Methods

Relation-ship

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

Security and Assurance Concerns in ISO



ISO

TMB

Advisory Group on Security

IEC

JTC 1 Information Technology

IEEE Computer Society

SC 7

Software and Systems Engineering

SC 22

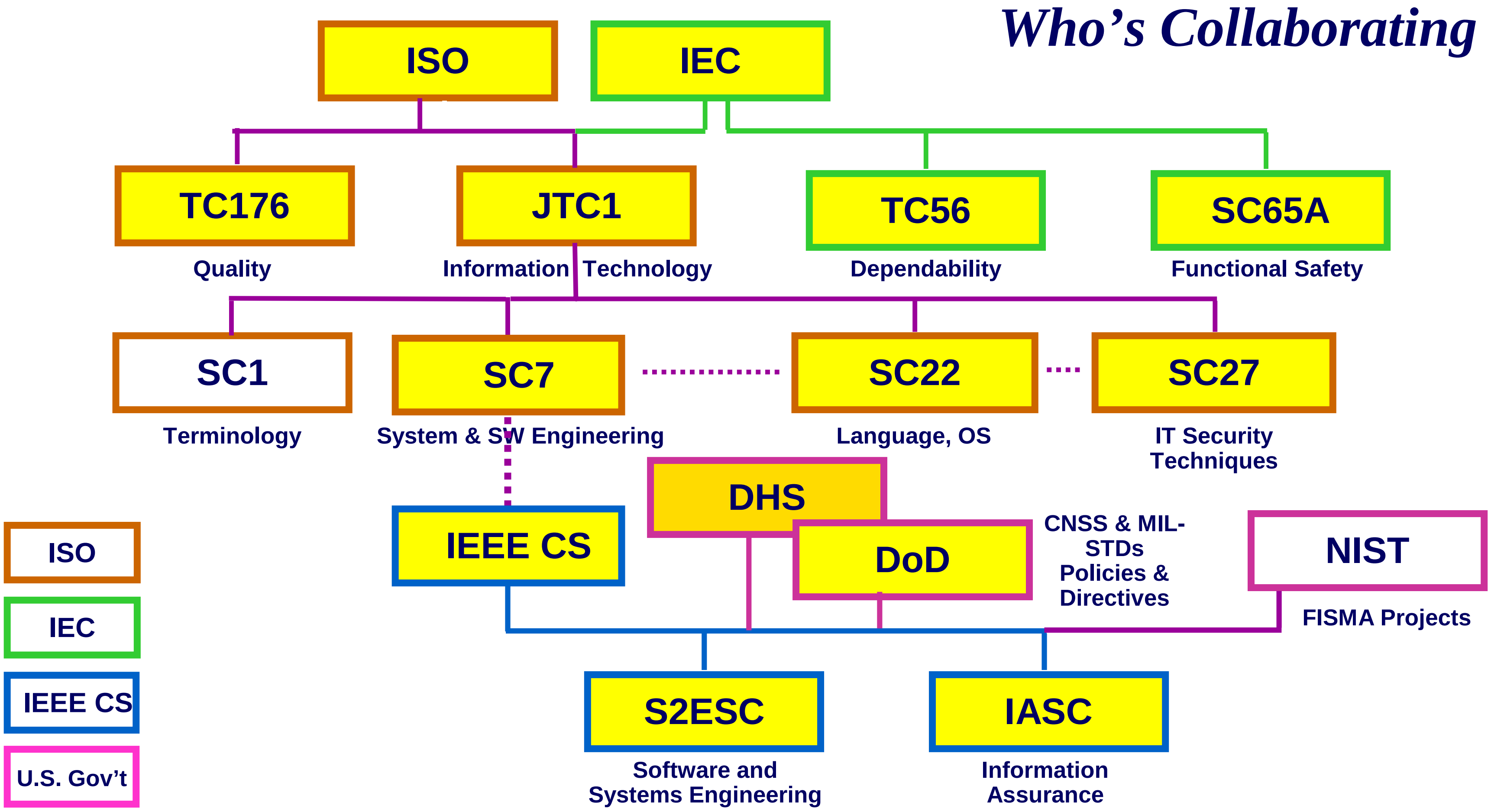
Programming Languages

SC 27

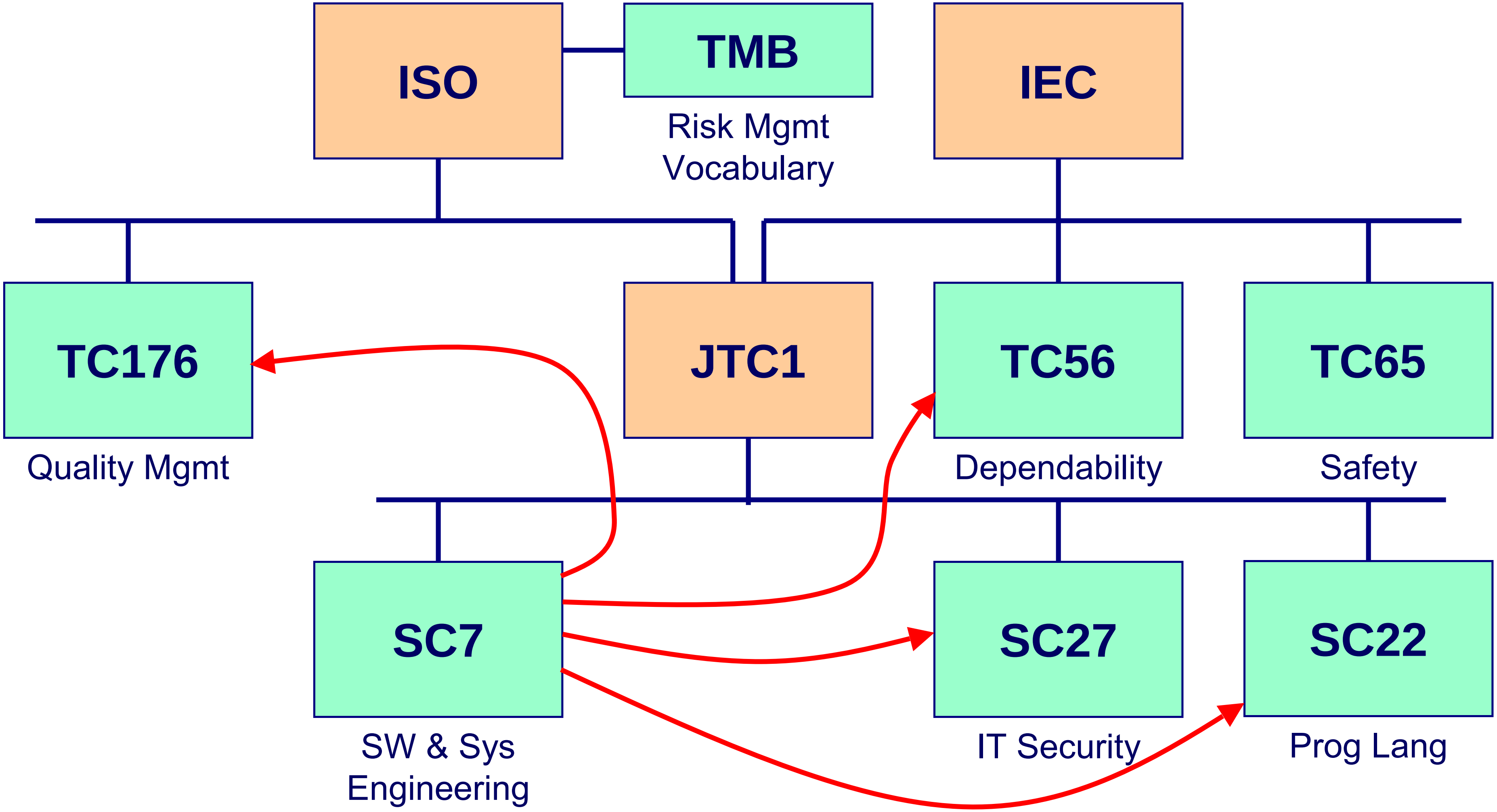
IT Security

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

Harmonization Efforts Impacting Systems and Software Assurance



Leveraging/Linking International Standards



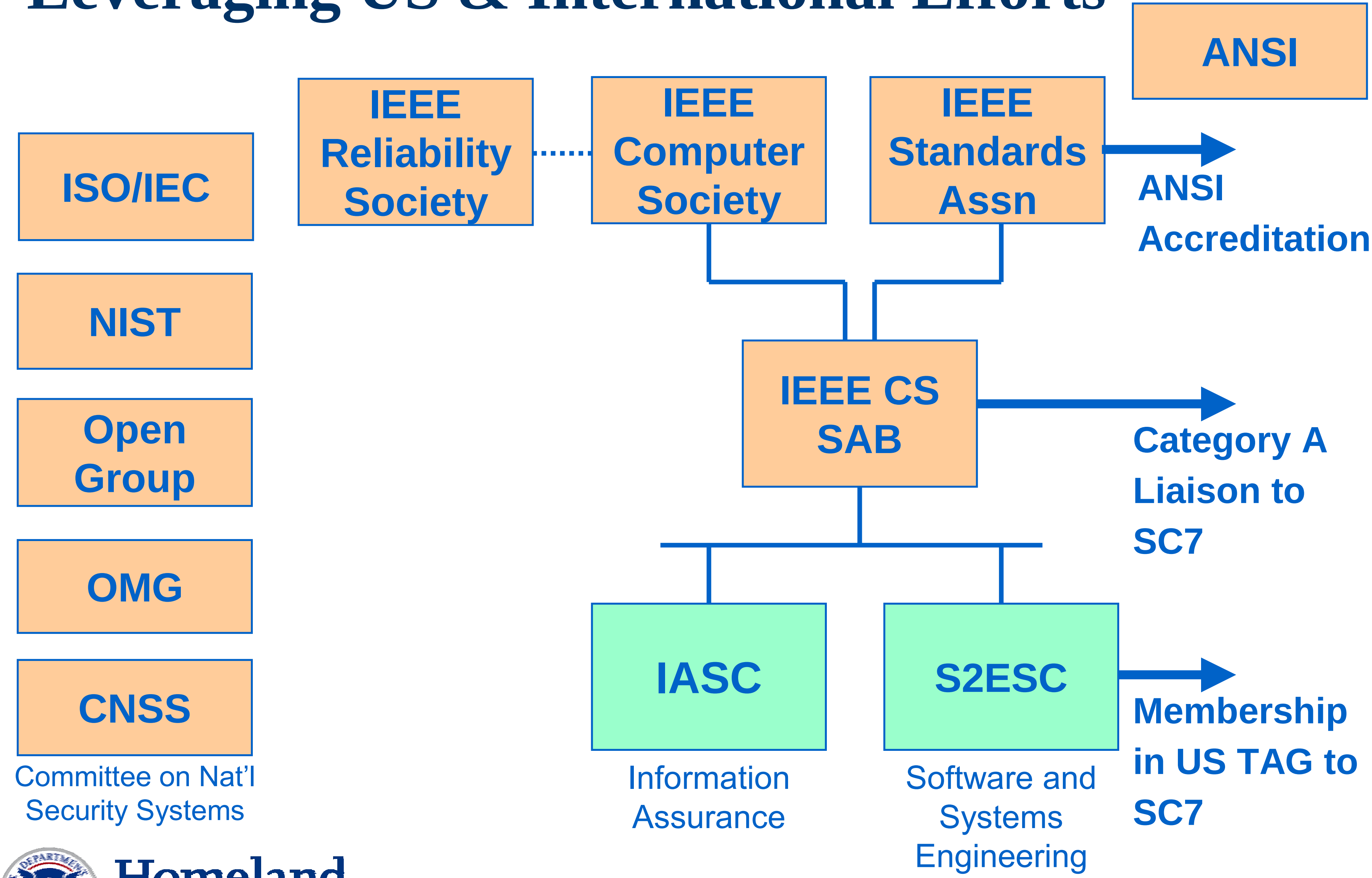
Homeland Security

*** DHS NCSD has membership on SC7 & SC27 along with FFRDC support serving in liaison role between SC7 & SC27**

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

Leveraging US & International Efforts



ANSI

ISO/IEC

NIST

Open Group

OMG

CNSS

Committee on Nat'l Security Systems

IEEE Reliability Society

IEEE Computer Society

IEEE Standards Assn

ANSI Accreditation

IEEE CS SAB

Category A Liaison to SC7

IASC

Information Assurance

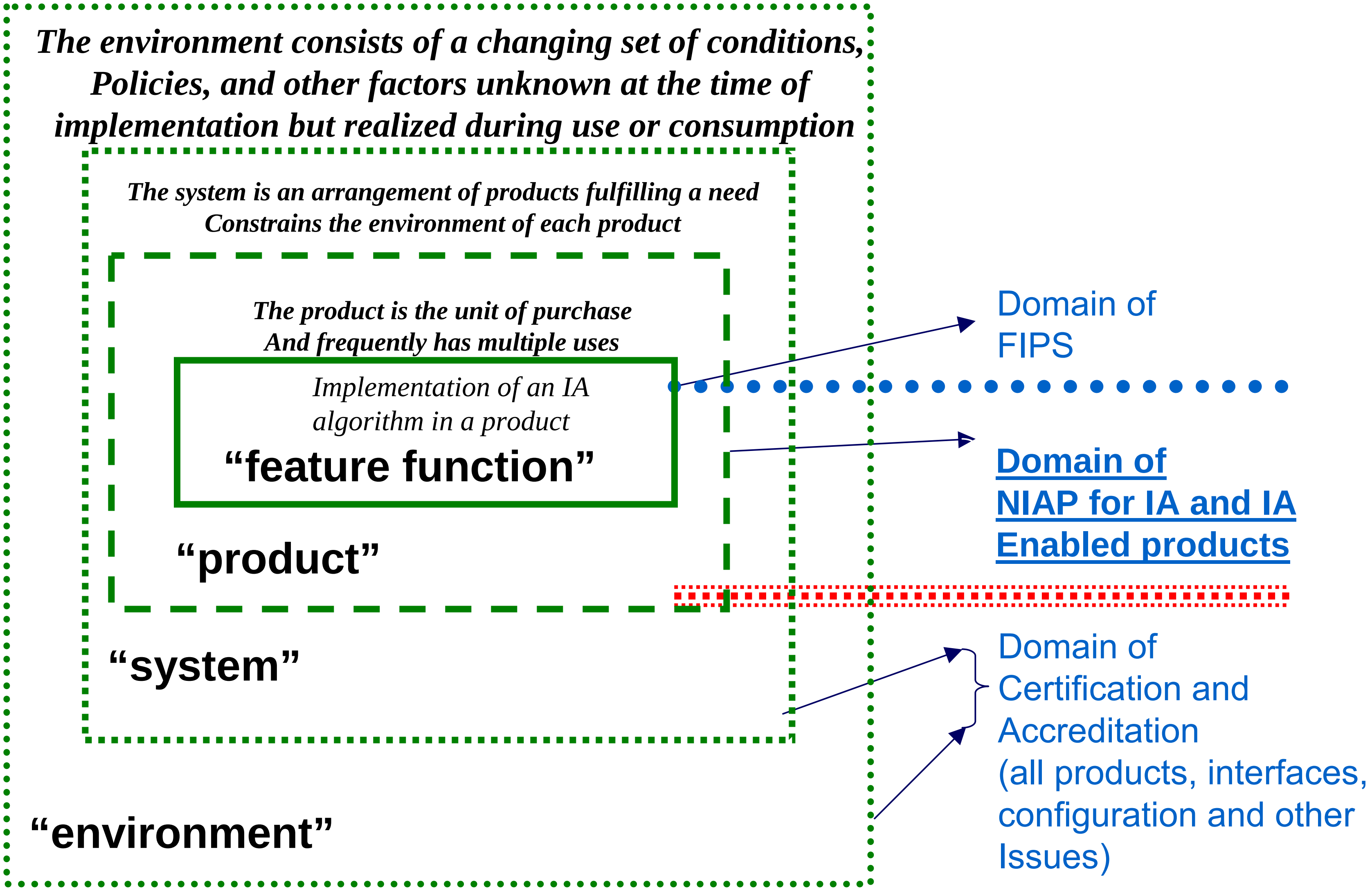
S2ESC

Software and Systems Engineering

Membership in US TAG to SC7

Homeland Security

Context for IT Security



The environment consists of a changing set of conditions, Policies, and other factors unknown at the time of implementation but realized during use or consumption

The system is an arrangement of products fulfilling a need Constrains the environment of each product

The product is the unit of purchase And frequently has multiple uses

Implementation of an IA algorithm in a product

"feature function"

"product"

"system"

"environment"

Domain of FIPS

Domain of NIAP for IA and IA Enabled products

Domain of Certification and Accreditation (all products, interfaces, configuration and other Issues)

Homeland Security

New 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 2005 presentation, “Best Practices for Delivering Safe, Secure, and Dependable Mission Capabilities”

Input to 15026 from the Safety and Security Extensions for Integrated CMMs

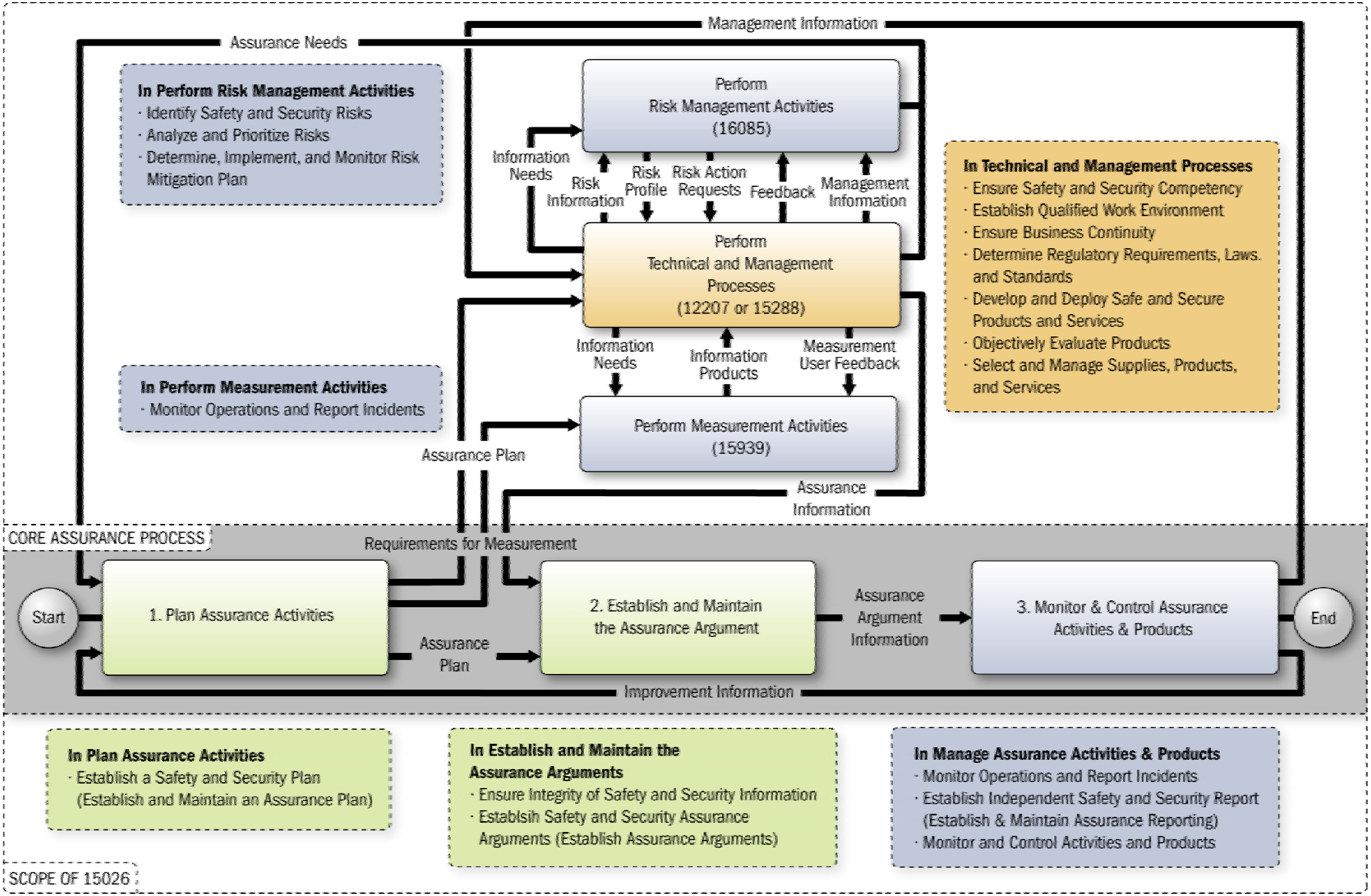
1. Ensure Safety and Security Competency
2. Establish Qualified Work Environment
3. Ensure Integrity of Safety and Security Information
4. Monitor Operations and Report Incidents
5. Ensure Business Continuity
6. Identify Safety and Security Risks
7. Analyze and Prioritize Risks
8. Determine, Implement, 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 Department of Defense and Federal Aviation Administration joint project on, Safety and Security Extensions for Integrated Capability Maturity Models, September 2004 www.faa.gov/ipg

From synthesis and harmonization of practices from 8 standards (4 on security and 4 on safety)

ISO/IEC 15026 Framework for System & SW Assurance



Management Information

Assurance Needs

In Perform Risk Management Activities
- Identify Safety and Security Risks
- Analyze and Prioritize Risks
- Determine, Implement, and Monitor Risk Mitigation Plan

Perform
Risk Management Activities
(16085)

Information Needs

Risk Information

Risk Profile

Risk Action Requests

Feedback

Management Information

Perform
Technical and Management
Processes
(12207 or 15288)

In Technical and Management Processes
- Ensure Safety and Security Competency
- Establish Qualified Work Environment
- Ensure Business Continuity
- Determine Regulatory Requirements, Laws. and Standards
- Develop and Deploy Safe and Secure Products and Services
- Objectively Evaluate Products
- Select and Manage Supplies, Products, and Services

Information Needs

Information Products

Measurement User Feedback

In Perform Measurement Activities
- Monitor Operations and Report Incidents

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

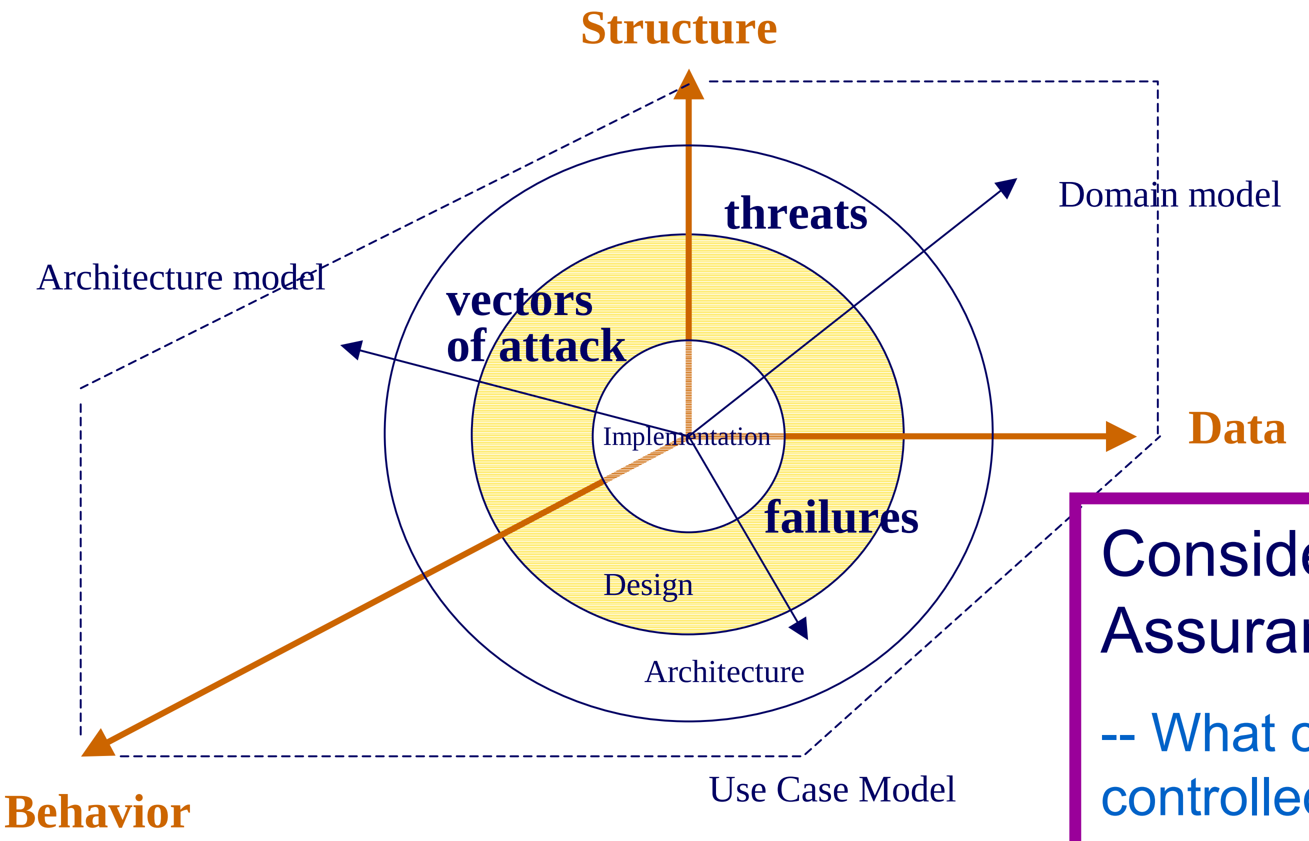
In Plan Assurance Activities
- Establish a Safety and Security Plan (Establish and Maintain an Assurance Plan)

In Establish and Maintain the Assurance Arguments
- Ensure Integrity of Safety and Security Information
- Establsih Safety and Security Assurance Arguments (Establish Assurance Arguments)

In Manage Assurance Activities & Products
- Monitor Operations and Report Incidents
- Establish Independent Safety and Security Report (Establish & Maintain Assurance Reporting)
- Monitor and Control Activities and Products

SCOPE OF 15026

Separation of Concerns in Software Systems



Considerations for Assurance Arguments:

-- What can be understood & controlled –vs- what cannot

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

Used to facilitate discussions in SwA WG on Practices and Processes, Aug 2005

Interoperability facilitates exchange

- In order to facilitate exchange of claims about software industry-wide, there should be (at least):
  - agreement of common terminology, boilerplate claims, properties, etc.
  - Structured way to exchange such claims (templates, XML schemas, etc.)
  - Archives of such claims (libraries, repositories) that allow search, comparison, etc. (which again needs shared taxonomy, etc.)
  - Agreed-upon ways to interpret such claims, properties, etc. (common meaning, as opposed to simply common format).
  - When it comes to software – all this needs to be automated (supported by tools)

Proposed standardization work within OMG

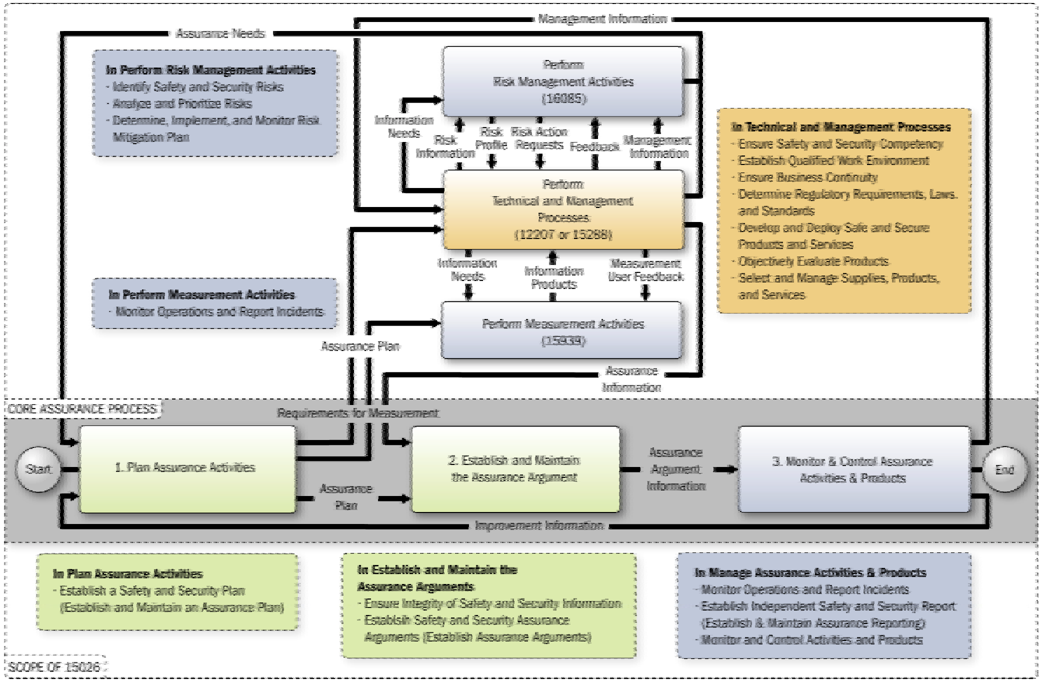
- Recently, OMG launched Architecture-Driven Modernization (ADM) Task Force to develop specifications related to modernization of existing software systems.
  - Often referred to as "*MDA-in-reverse,*" it addresses the need to apply modeling techniques to software products that are already in production to facilitate understanding, evaluation, assessment, certification, or modernization.
  - ADM techniques reach new frontiers in software understanding.
- The first specification of the ADM Task Force – Knowledge Discovery Meta-model (KDM) - establishes the Foundation for Software Assurance and Modernization by standardizing common platform-neutral framework for describing software systems, their artifacts, designs, architecture and their operating environment.
  - KDM defines common terminology that can be shared by tool vendors and integrators, and assessment and certification bodies;
  - KDM also defines a formal interoperability specification, so that descriptions can be exchanged; thus it providing interoperability in software understanding.

Software Assurance Meta-model

- Process of building *trust* … embodied in software asset evaluation
- *Claims* about software systems…
  - Involve certain *Target Requirement* (intentions)
    - Related to *risks*
    - How vendor-specified risk is mitigated
    - Security requirements
    - Process requirements (cleanroom, ISO, etc.;)
    - Architectural TR (especially when system of systems; integrations of 3rd party components is involved)
  - Specify the *degree* to which the target requirement was addressed
  - Levels of *certainty* of the claim
  - What kind of proof exists to support the certain claim
  - What benchmarks were involved
- *Process* of building/assembling software components
- Trust is *derived* from claims
  - *Levels* of trust and how vendor-specified risks *match* buyer's risks

Next Steps for System and Software Assurance

- Modify 15026 context diagram
- Write supporting text
  - Clearly establish centrality of the Assurance Argument
  - Describe the Assurance Argument in detail
  - Describe interfaces/ amplifications to the Technical and Management processes of 15288 and 12207
  - Describe interfaces/ amplifications to the Risk Management Process of 16085 and the Measurement Process of 15939 and Security Metrics of 27004
- Reconvene in December to review and comment



In Perform Risk Management Activities
- Identify Safety and Security Risks
- Analyze and Prioritize Risks
- Determine, Implement, and Monitor Risk Mitigation Plan

In Perform Measurement Activities
- Monitor Operations and Report Incidents

Perform Risk Management Activities (16085)

Perform Technical and Management Processes (12207 or 15288)

Perform Measurement Activities (15939)

In Technical and Management Processes
- Ensure Safety and Security Competency
- Establish Qualified Work Environment
- Ensure Business Continuity
- Determine Regulatory Requirements, Laws, and Standards
- Develop and Deploy Safe and Secure Products and Services
- Objectively Evaluate Products
- Select and Manage Supplies, Products, and Services

CORE ASSURANCE PROCESS

Start

1. Plan Assurance Activities

2. Establish and Maintain the Assurance Argument

3. Monitor & Control Assurance Activities & Products

End

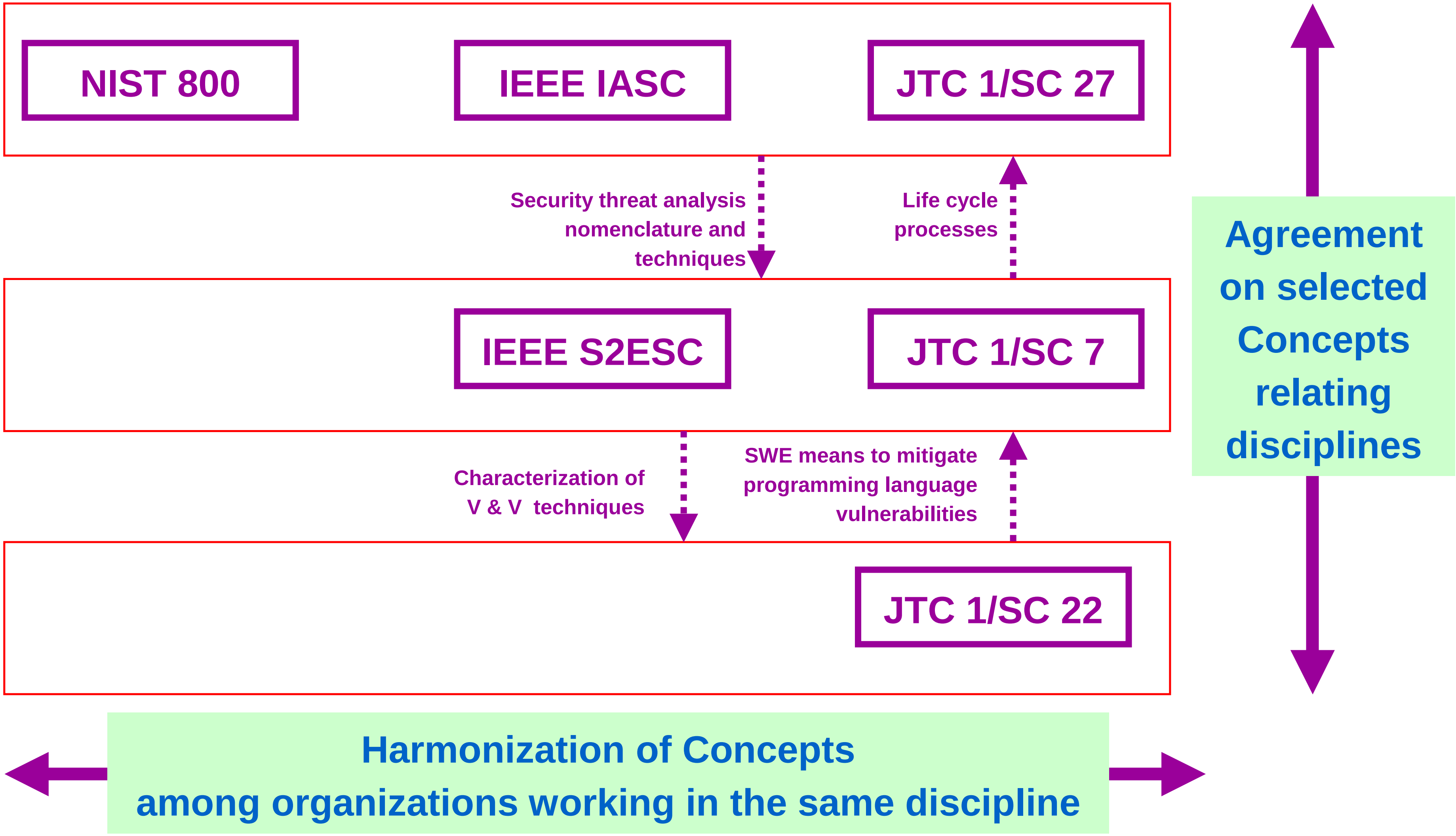
In Plan Assurance Activities
- Establish a Safety and Security Plan (Establish and Maintain an Assurance Plan)

In Establish and Maintain the Assurance Arguments
- Ensure Integrity of Safety and Security Information
- Establsih Safety and Security Assurance Arguments (Establish Assurance Arguments)

In Manage Assurance Activities & Products
- Monitor Operations and Report Incidents
- Establish Independent Safety and Security Report (Establish & Maintain Assurance Reporting)
- Monitor and Control Activities and Products

SCOPE OF 15026

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

Key Standards for Software & 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
  - Describes 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

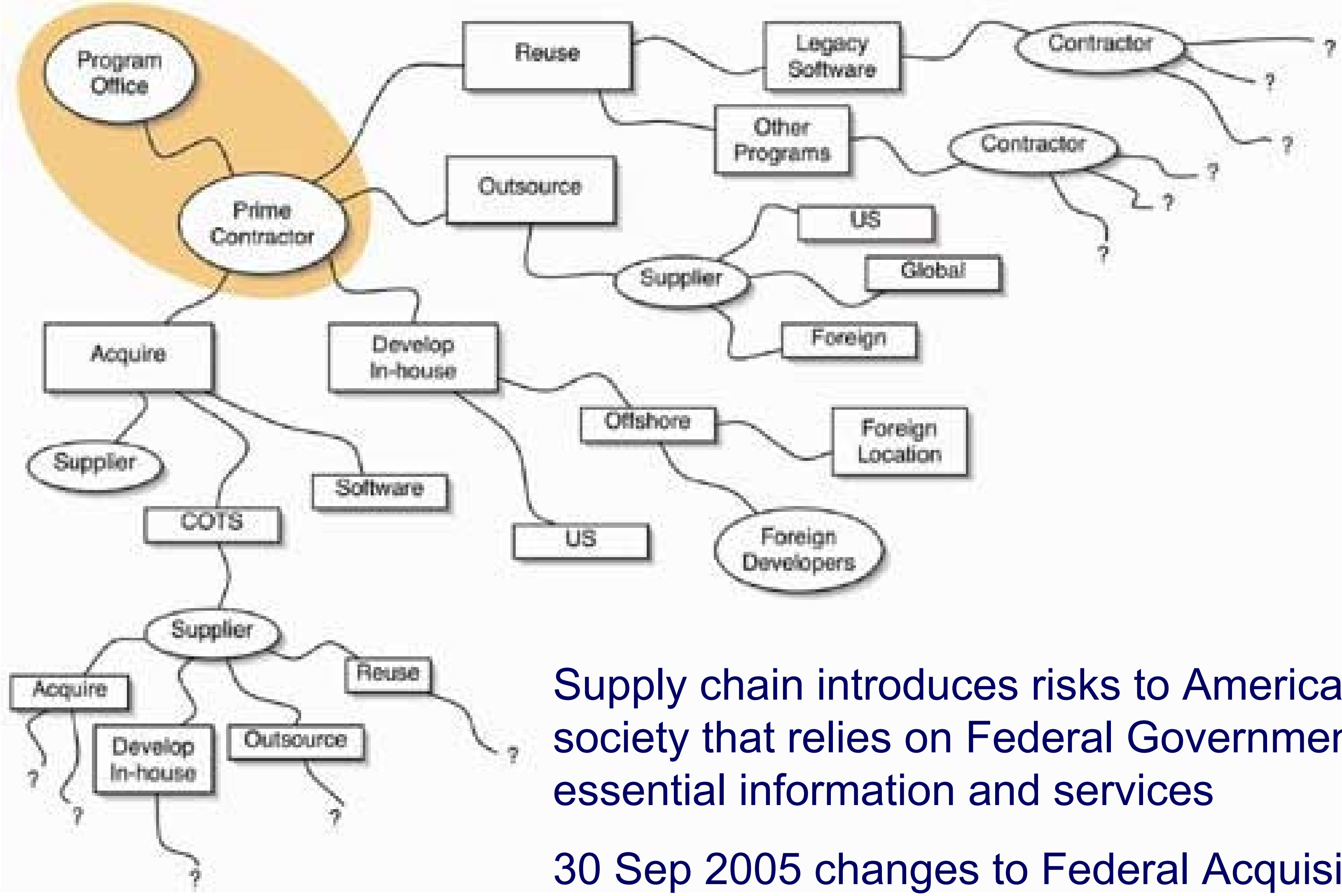
Some Current Efforts

- ISO 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.
- ISO SC22
  - Develop coding guidelines for common programming languages.
- ISO SC27
  - Expand their perceived context to include assurance concerns.
- IEEE S2ESC
  - Use as an “integrator” of standards for packaging and transition to industry.

Software Assurance: Acquisition

- **Collaborate with stakeholders to 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
  - Work with organizations providing acquisition training and education to develop applicable curriculum
  - Chair IEEE CS S2ESC WG to update of IEEE 1062, “Software Acquisition”
  - Collaborate with stakeholder organizations to support acquisition community:
    - 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
    - Develop and disseminate acquisition guidebook on acquisition of secure software-intensive systems and services
  - Collaborate with agencies implementing changes responsive to changes in the FAR that incorporated IT security provisions of FISMA when buying goods and services

**NCSD Goal Action 2.3.4



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

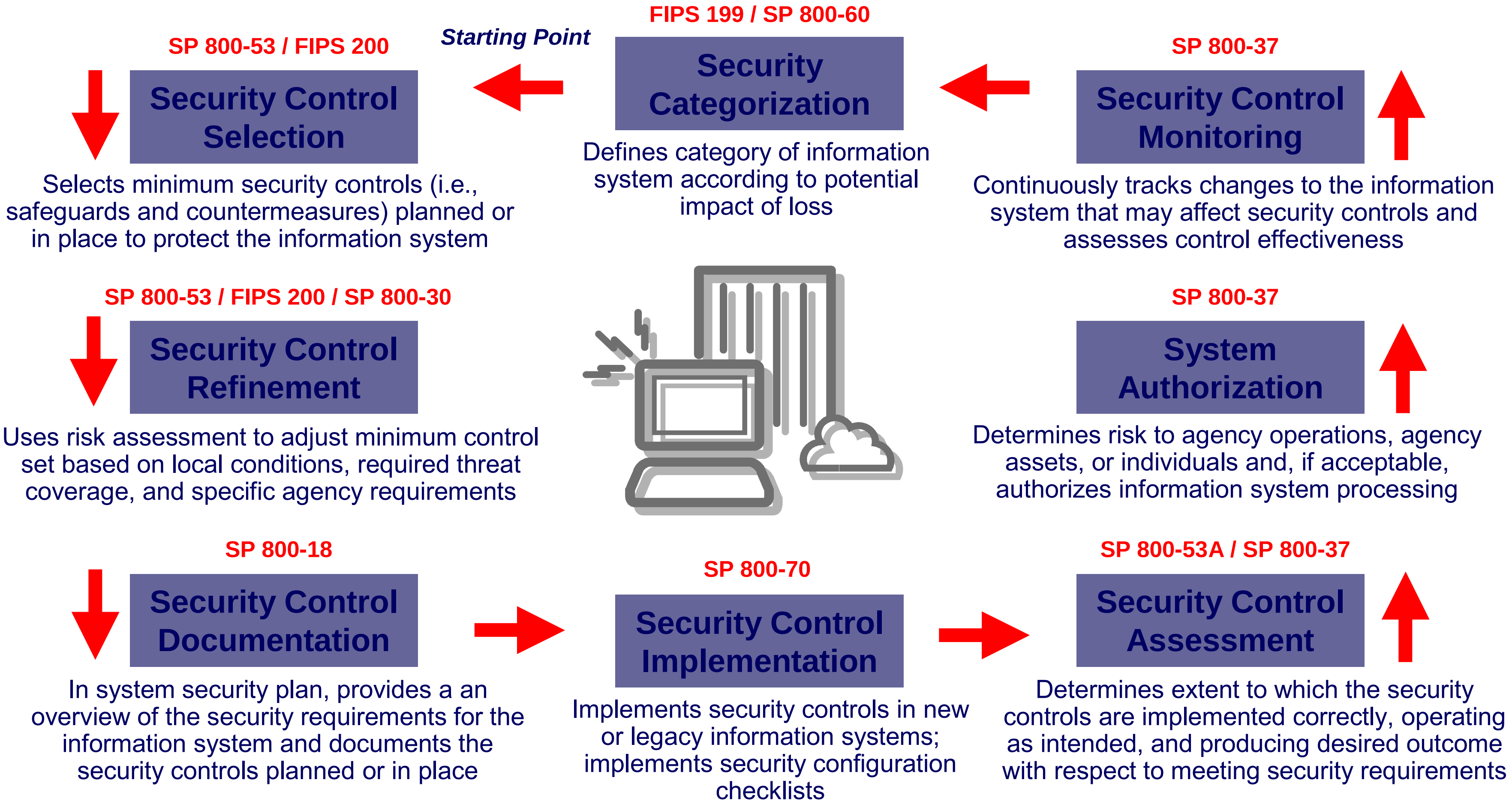
Focuses on the role of contractors in security as Federal agencies outsource various IT functions.

Homeland Security

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
  - Incorporate FISMA into Fed 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

NIST Enterprise Risk Management Framework



Starting Point

FIPS 199 / SP 800-60

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 800-53 / 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 800-18

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

SP 800-37

System Authorization

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

SP 800-37

Security Control Monitoring

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

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

Software Assurance: Technology

- Enhance software security measurement, identify SwA R&D priorities, and assess Software Assurance testing and diagnostic capabilities**
  - 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
    - NIST SEMATE workshops to assess, measure, and validate tool effectiveness
  - Identify R&D requirements for DHS S&T consideration; coordinating Software Assurance R&D requirements with other federal agencies
    - Advocate funding of R&D (through the DHS S&T Directorate) that will examine tools and techniques for analyzing software to detect security vulnerabilities.
    - Leverage SwA R&D prioritization efforts from DoD SwA Initiative (IRC HP list)
    - Leverage multi-agency Cyber Security and IA R&D provided to stakeholders.
    - Include techniques that require access to source code & binary-only techniques
  - Collaborate with other agencies and allied organizations to mature measurement in security to support SwA requirements and explore needs and organizing mechanisms for federated labs to address R&D needs

**NCSD Goal Action 2.3.3

Software Assurance (SwA) Outreach Service

- Co-sponsor semi-annual Software Assurance Forum for government, academia, and industry to facilitate the ongoing collaboration -- next 16-17 March 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

SPECIAL ISSUE: ENSURING SECURE SOFTWARE
CROSSTALK
SOFTWARE SECURITY
SoftwareTech NEWS
Secure Software Engineering
Homeland Security
Software Assurance Program
http://BuildSecurityIn.us-cert.gov

Homeland Security

Examining IT Security Requirements

- How are common flaws (vulnerabilities) in software addressed in procurements?
- Are existing schemes for product evaluation adequate?
- What test guidance should be provided?
- How should certification and accreditation processes better address security requirements?
- How does acquisition community evaluate capabilities of suppliers to deliver secure software?

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 SW Engineering 2004 curriculum

ABET

University acceptance

Professional Development

- Continuing Education
- Certification

CSDP Online Prep Course

IEEE CS SWE Book Series

Certified Software Development Professional

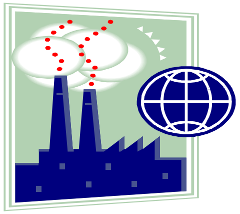
Individual acceptance

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

Homeland Security

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

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."

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
  - Security requirements need to be addressed along with other functions
  - Software assurance education and training curriculum 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, Federal agencies need to focus on software assurance as a means of better enabling operational resiliency

Next Software Assurance Forum at McLean Hilton 16-17 March 2006

www.us-cert.gov →

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Publications
Events
Other Resources
About Us

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.

Reporting

Announcements

Build Security In

Direct Links
National Cyber Alert System
Technical Security Alerts
Current Activity
Latest Version
Vulnerability Resources
New and Notable Vulnerabilities

http://buildsecurityin.us-cert.gov

Sponsored by DHS National Cyber Security Division

Build Security In

Home | Articles | Forums | Events | Additional Resources | About Us | FAQs | Feedback

Login: Username: Password: Login [Register] Quick Search: Search Advanced Search

Articles
What's New
Top Viewed Articles

Articles by Category
Best Practices
Architectural Risk Analysis
Assembly, Integration & Evolution
Code Analysis
Deployment and Operations
Incident Management
Measurement
Penetration Testing
Project Management
Requirements Engineering
Risk Management
Security Testing
Threat Modeling
Training & Awareness
White Box Testing

Knowledge
Attack Patterns
Business Relevance
Coding Practices
Coding Rules
Guidelines
Historical Risks
Principles
SDLC Process

Tools
Black Box Testing
Code Analysis
Modeling Tools

Getting Started with Build Security In

The articles have been grouped in a process agnostic view. The Content Areas are classified in the following sections: Architectural & Design, Code, Test, Requirements, System, and Fundamentals. Click Here to Learn More...

"Many security incidents are the result of exploits against defects in the design or code of software. The approach most commonly employed to address such defects is to attempt to retroactively bolt on devices that make it more difficult for those defects to be exploited. This is not a solution that gets to the root cause of the problem and threat."
- CERT® Coordination Center (CERT/CC) of the Carnegie Mellon® Software Engineering Institute (SEI).

What is "Build Security In" (BSI)?

Build Security In is a project of the Strategic Initiatives Branch of the National Cyber Security Division (NCSD) of the Department of Homeland Security (DHS). The Software Engineering Institute (SEI) was engaged by the NCSD to provide support in the Process and Technology focus areas of this initiative. The SEI team will develop and collect software assurance and software security information that will help software developers, architects, and security practitioners to create secure systems. Click Here to Learn More...

How Can I Collaborate?

If you are new to the site, you will want to register to collaborate with other developers faced with the challenges of developing secure code. Click Here to Register Now...

What's New

Source Code Analysis Tools - Overview

A security analyzer is an automated tool for helping analysts find security-related problems in software. Modern security analyzers focused on building security in analyze software source code, trying to automate some of the tasks that a human analyst might perform.

Source Code Analysis Tools ? Business Case

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

Homeland Security

Homeland Security

Questions?

Back-up Slides

Vulnerabilities and Malware

- **Vulnerability information**
  - **National Vulnerability Database (NVD)** **http://nvd.nist.gov**

    Search U.S. government vulnerability resources for information about vulnerabilities on your systems
  - **Common Vulnerabilities and Exposures List (CVE)** **http://cve.mitre.org**

    Search vulnerabilities by CVE name or browse the US-CERT list of vulnerabilities in CVE name order
  - **Open Vulnerability Assessment Language (OVAL)** **http://oval.mitre.org**

    Identify vulnerabilities on your local systems using OVAL vulnerability definitions

- **Malware**
  - **Common Malware Enumeration (CME)** **http://cme.mitre.org**

    Provides single, common identifiers to new virus threats to reduce public confusions during malware outbreaks.

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 vulnerability resource tool co-sponsored by NIST and the DHS National Cyber Security Division/US-CERT, and it:

- 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

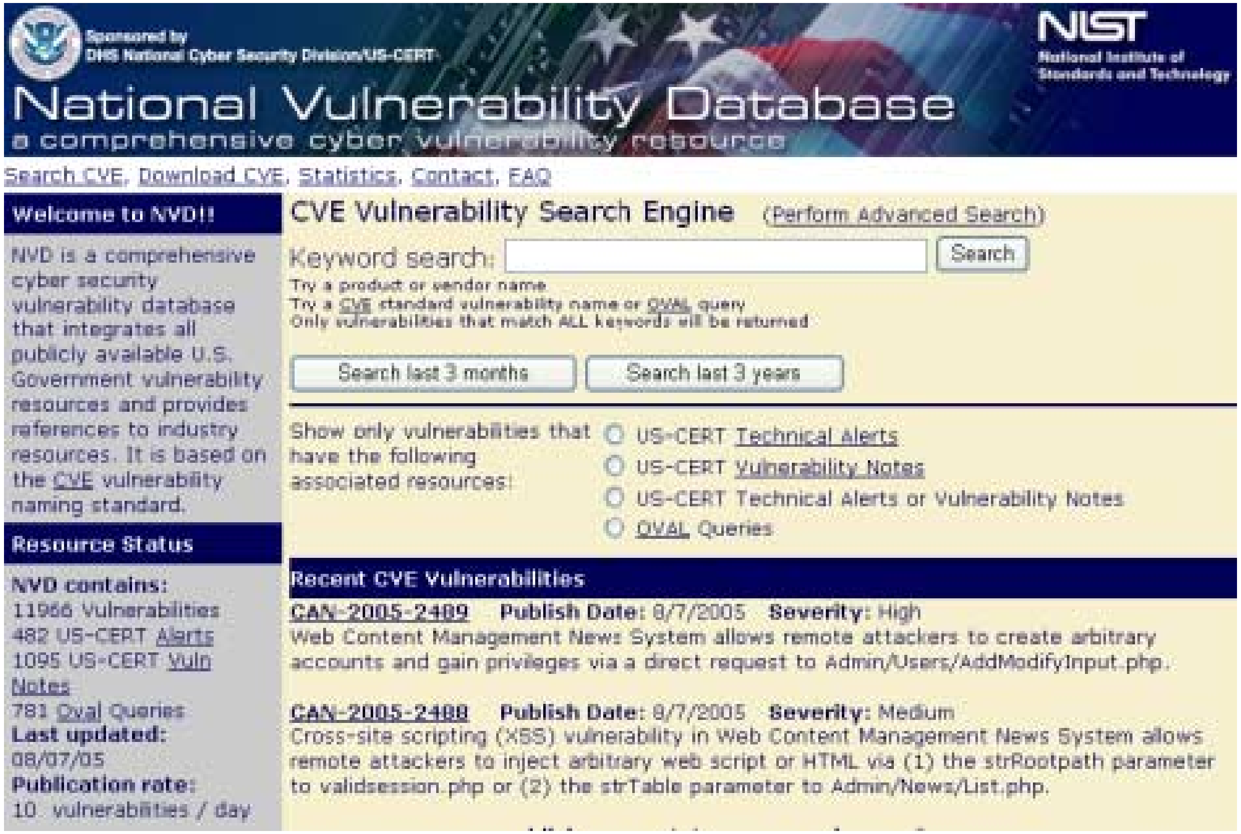
NVD Search Capability

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 12,800 vulnerability summaries
- 38 US-CERT Alerts
- 1090 US-CERT Vulnerability Notes
- Over 1,000 OVAL queries
- 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

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: [ ] 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

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

- 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 http://cve.mitre.org

http://cve.mitre.org/

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

GET CVE
View | Search | Download

CVE HOME
ABOUT CVE
NEWS AND EVENTS
PRESS VIEW
COMPATIBLE PRODUCTS
EDITORIAL BOARD
ADVISORY COUNCIL
FREE NEWSLETTERS
CONTACT US
INDEX

US-CERT
www.us-cert.gov

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

[illegible]

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

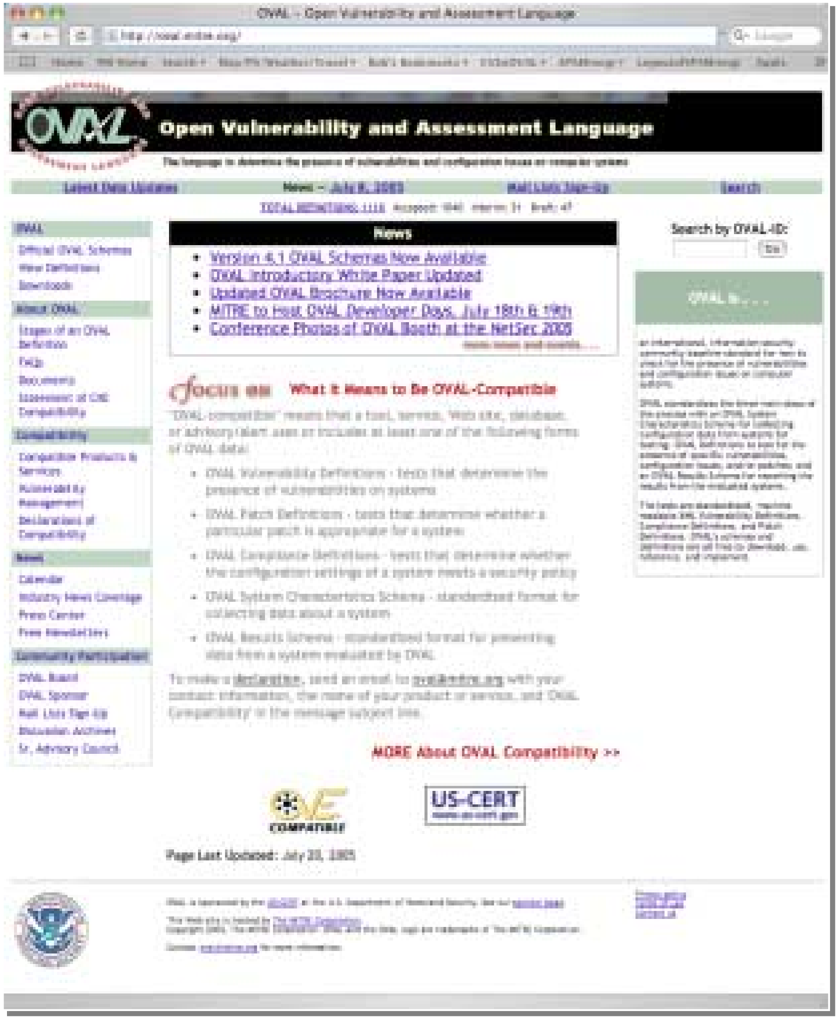
[illegible]

Total Unique CVE Names: 9529
Current CVE Version: 20040901

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

Open Vulnerability and Assessment Language

- 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



OVAL - Open Vulnerability and Assessment Language

http://oval.mitre.org/

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: 1,141 Accepted: 1040 Interim: 31 Draft: 47

OVAL
- Official OVAL Schemas
- View Definitions
- Downloads

About OVAL
- Stages of an OVAL Definition
- FAQs
- Documents
- Assessment 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 >>

Search by OVAL-ID: Go

OVAL is . . .

[illegible]

US-CERT

Page Last Updated: July 20, 2005

[illegible]

1,141 OVAL Definitions

http://oval.mitre.org

Public unveiling - December 2002

CME Common™ Malware Enumeration

Reducing Public Confusion During Malware Outbreaks

http://cme.mitre.org

CME provides single, common identifiers to new virus threats to reduce public confusions during malware outbreaks.

- **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**

CME is not an attempt to solve the challenges involved with naming schemes for viruses and other forms of malware, but instead aims to facilitate the adoption of a shared, neutral indexing capability for malware. The CME initiative seeks to:

-- Reduce the public's confusion in referencing threats during malware incidents.

-- Enhance communication between anti-virus vendors.

-- Improve communication and information sharing between anti-virus vendors and the rest of the information security community.

US-CERT Publications on Securing Computers

- **Before You Connect a New Computer to the Internet**
  - Tips for first time connecting a new (or newly upgraded) computer to the internet
  - For home users, students, small businesses, or any organizations with limited Information Technology (IT) support

- **Home Network Security**
  Overview of security risks and countermeasures associated with internet connectivity

- **Home Computer Security**
  Examples, checklists, and a glossary for securing a home computer

- **Common Sense Guide to Cyber Security for Small Businesses**
  - Security practices for non-technical managers at companies with more than a single computer, but without a sophisticated in-house information technology department
  - Details of small businesses that were adversely affected by cyber crimes

- **Virus Basics**
  An introduction to viruses and ways to avoid them

- **Software License Agreements: Ignore at Your Own Risk**
  An overview of the risks computer users may incur by blindly agreeing to terms contained in software licensing agreements.