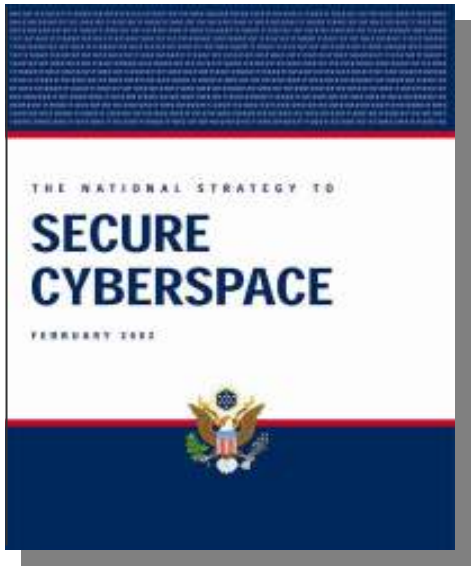
Software Assurance:

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



Considerations in Advancing the National Strategy to Secure Cyberspace

July 12, 2006

Homeland Security

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

What if…

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

Homeland Security

National Strategy for Homeland Security

"We will **lead the unified national effort to secure America**. We will **prevent and deter terrorist attacks and protect against and respond to threats and hazards to the nation**. We will ensure safe and secure borders, welcome lawful immigrants and visitors, and **promote the free-flow of commerce**."

Key Objective I	Key Objective II	Key Objective III
Prevent terrorist attacks within the United States	Reduce America's vulnerability to terrorism	Minimize the damage and recover from attacks that do occur

Authorization: Homeland Security Act of 2002 at Title 6, U.S. Code

Homeland Security

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

- Chemical Industry
  - 66,000 chemical plants

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

- Water
  - 1,800 federal reservoirs
  - 1,600 treatment plants
- Public Health
  - 5,800 registered hospitals

- Postal and Shipping
  - 137M delivery sites

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

- Telecomm
  - 2B miles of cable

- Energy
  - 2,800 power plants
  - 300K production sites

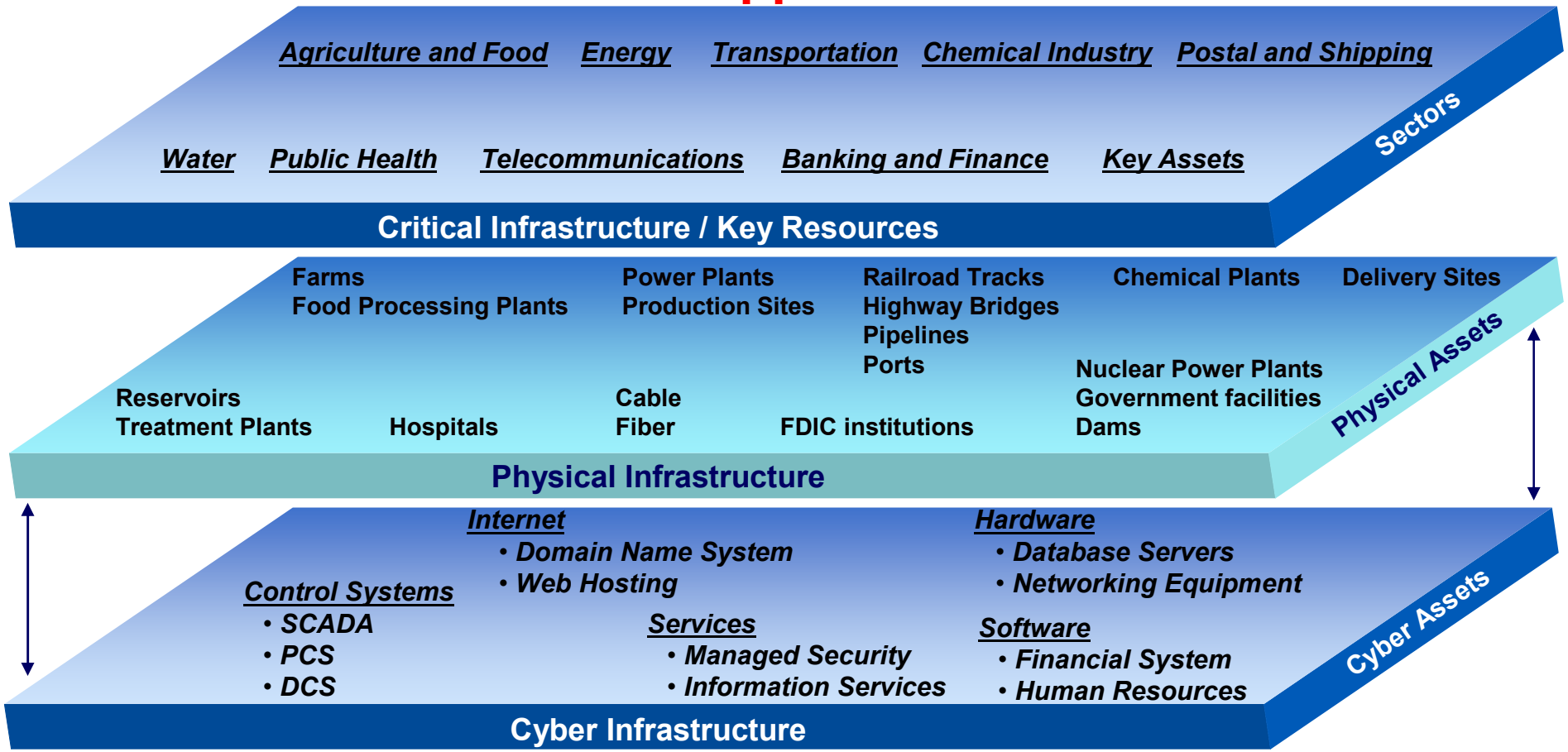
- Key Assets
  - 104 nuclear power plants
  - 80K dams
  - 5,800 historic buildings
  - 3,000 government facilities
  - commercial facilities / 460 skyscrapers

Homeland Security

An Asymmetric Target-rich Environment

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

Need for secure software applications



Homeland Security

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

Cyber-related Disruptions and the Economy

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

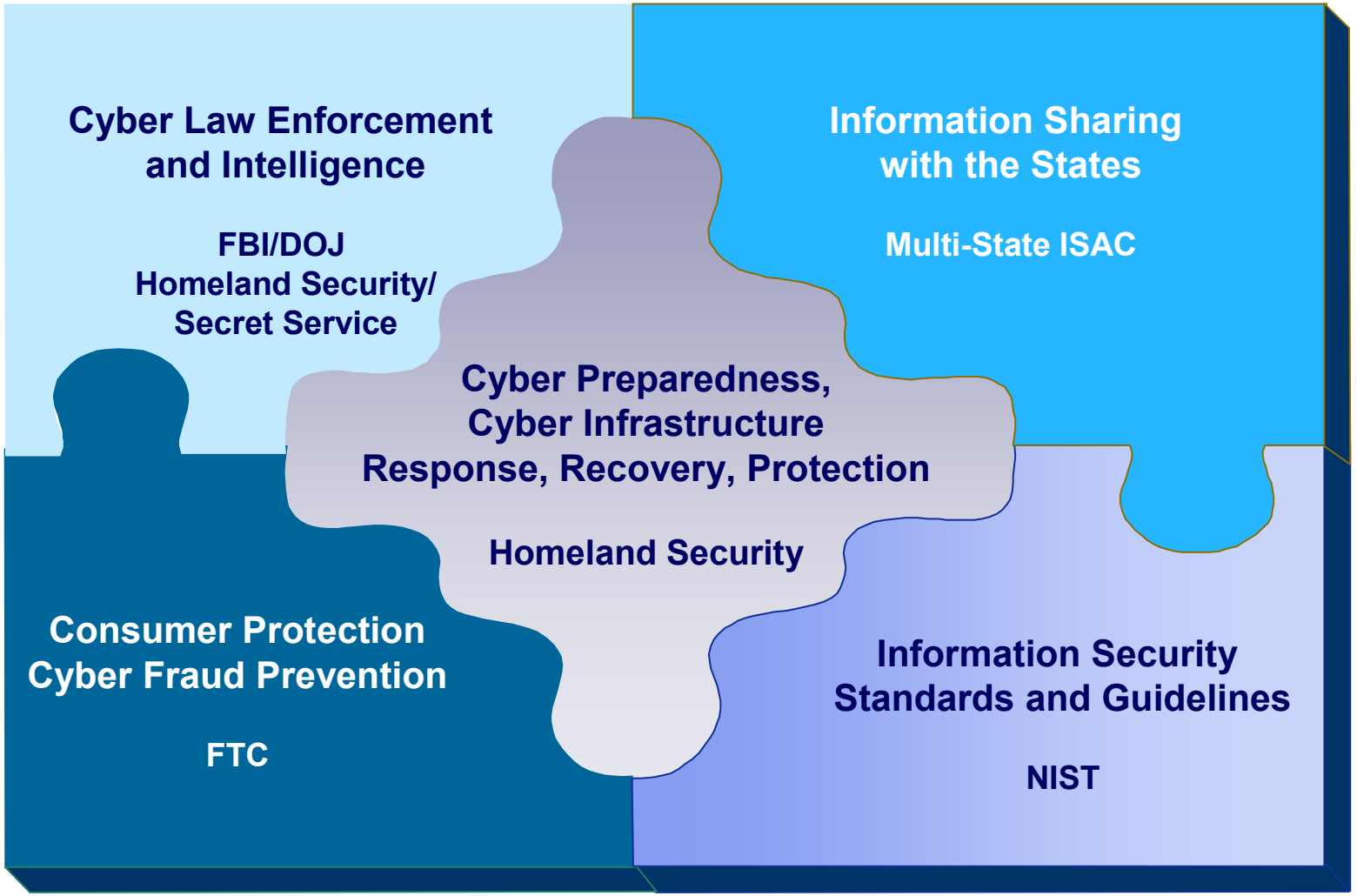
Business Losses and Damages

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

Homeland Security

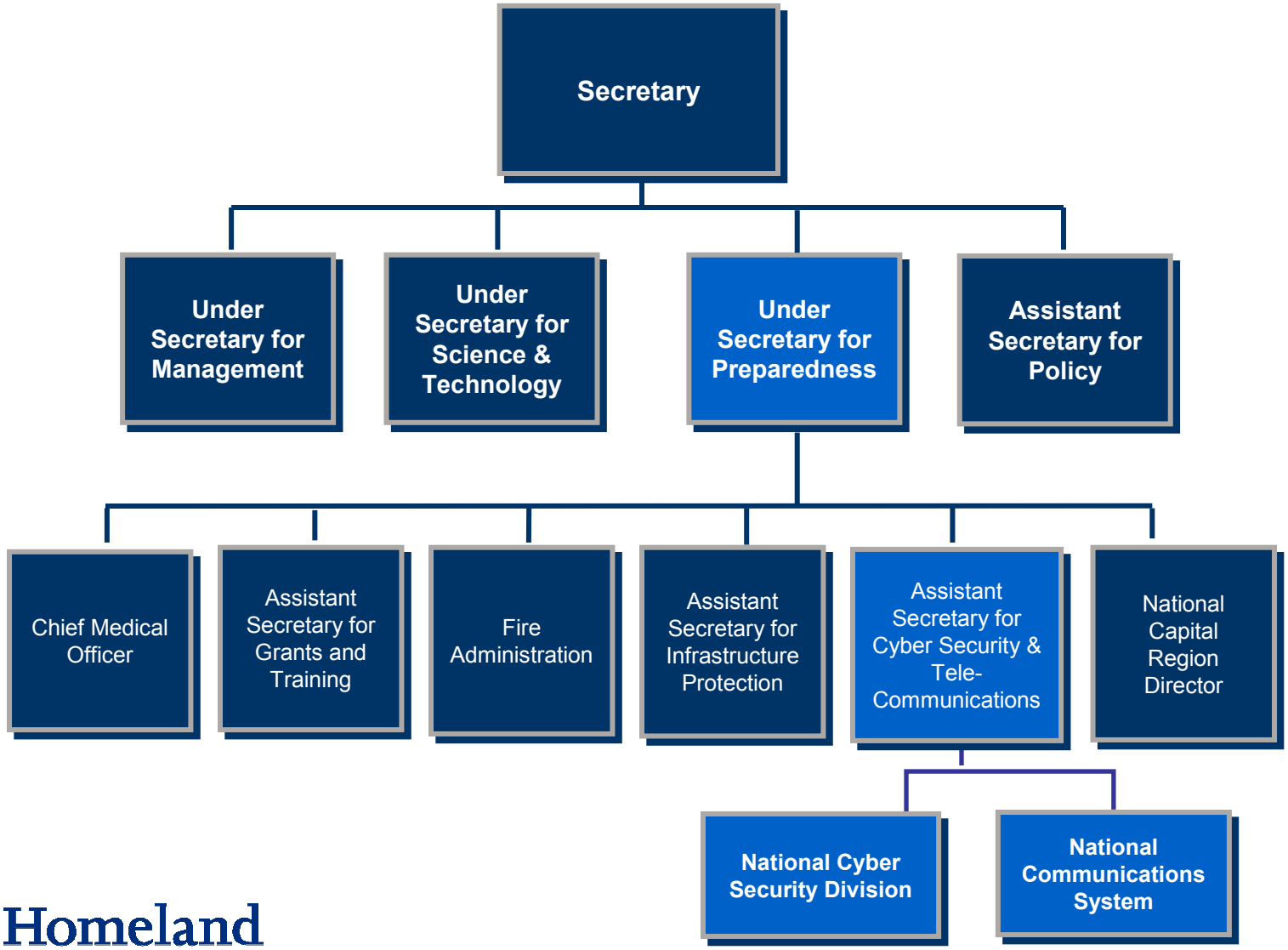
Impact of Spyware not fully known

Government plays key cyber security roles



Homeland Security

DHS and the National Cyber Security Division



Homeland Security

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

Cyber Preparedness

The National Cyber Security Division (NCSD) mission is to work collaboratively with public, private, and international entities 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

Overarching Priorities:

- National Cyber Security Response System
- Cyber Risk Management

Homeland Security

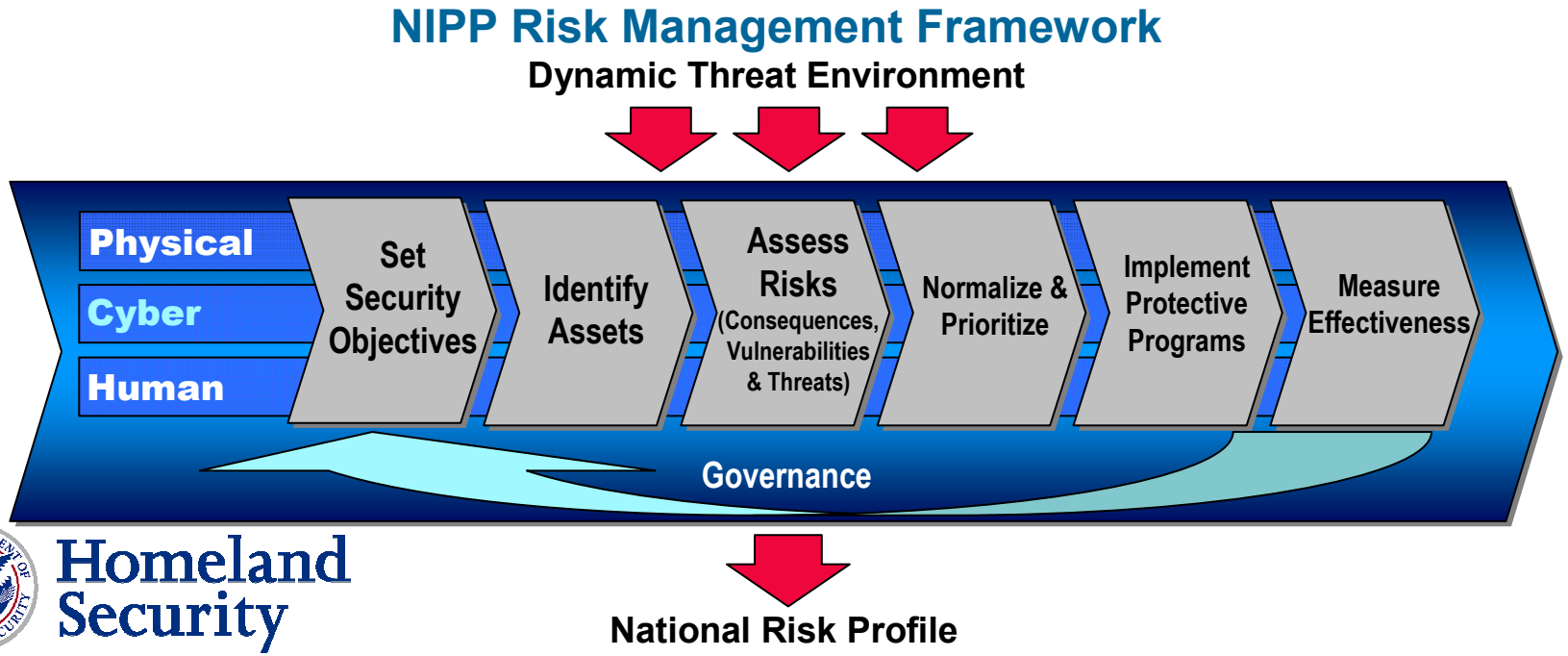
HSPD-7: A national policy to protect our nation's infrastructure

- 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

Homeland Security

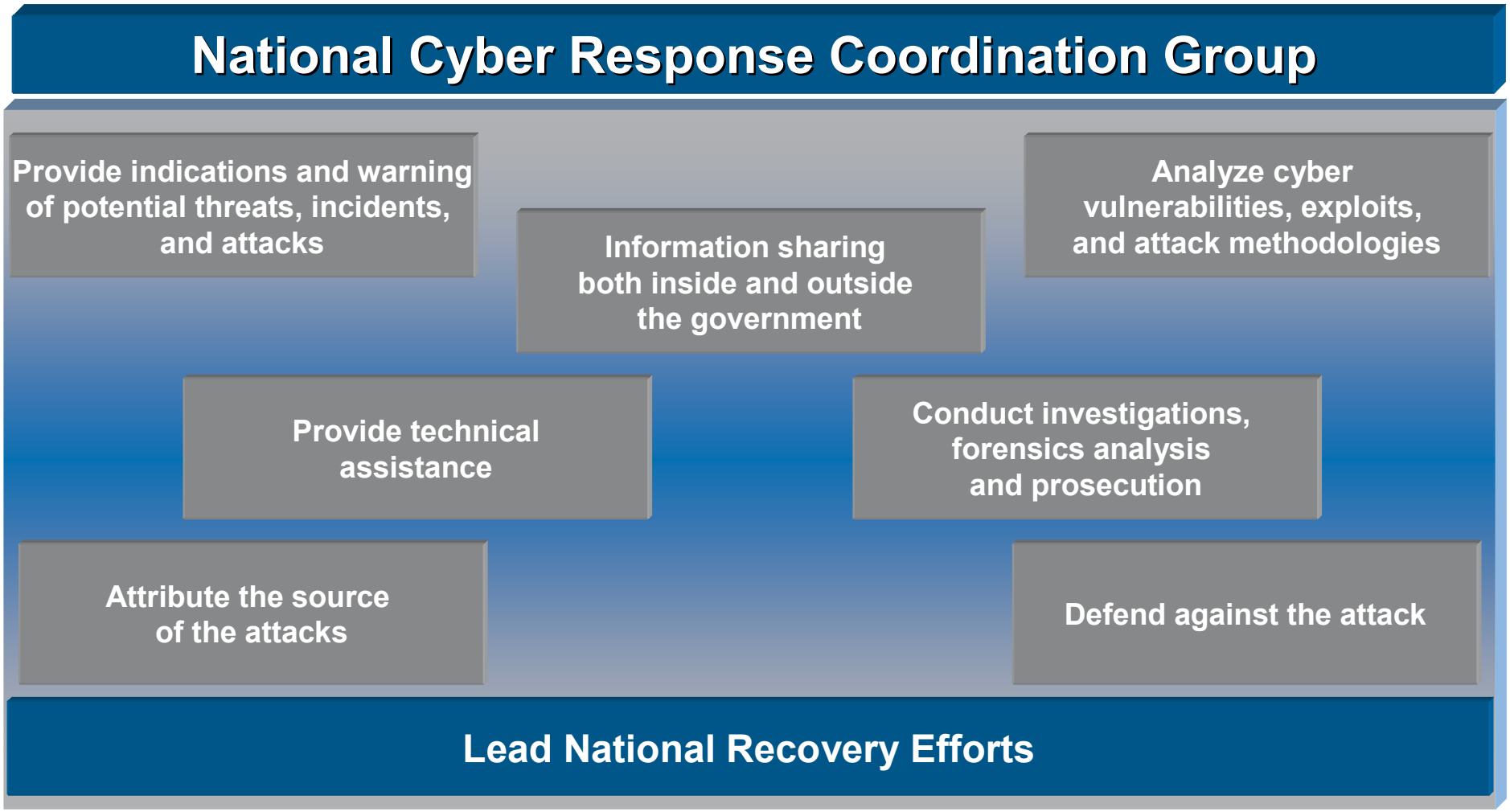
The NIPP outlines a unifying structure

- 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



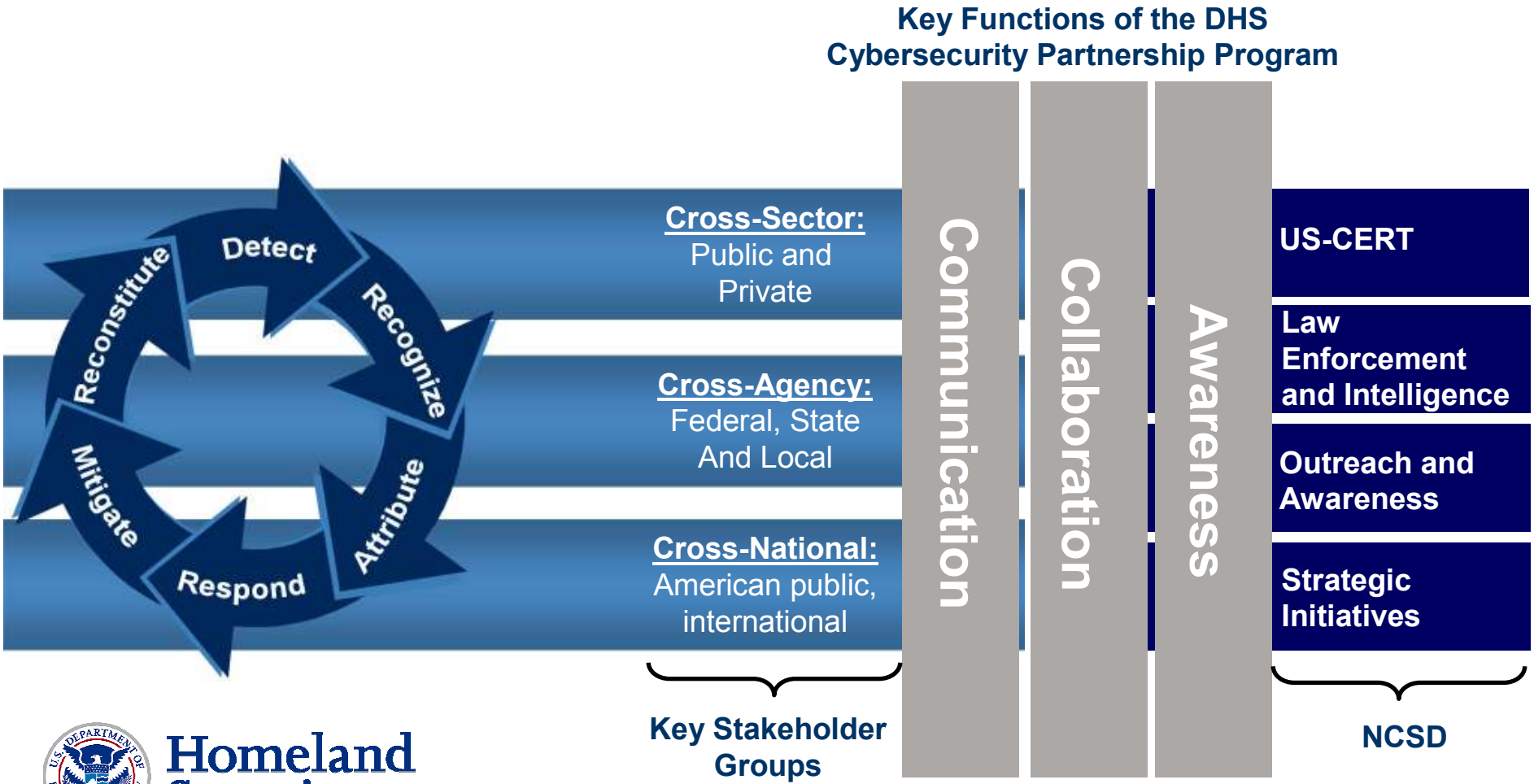
Homeland Security

NRP Cyber Annex describes the framework for response coordination



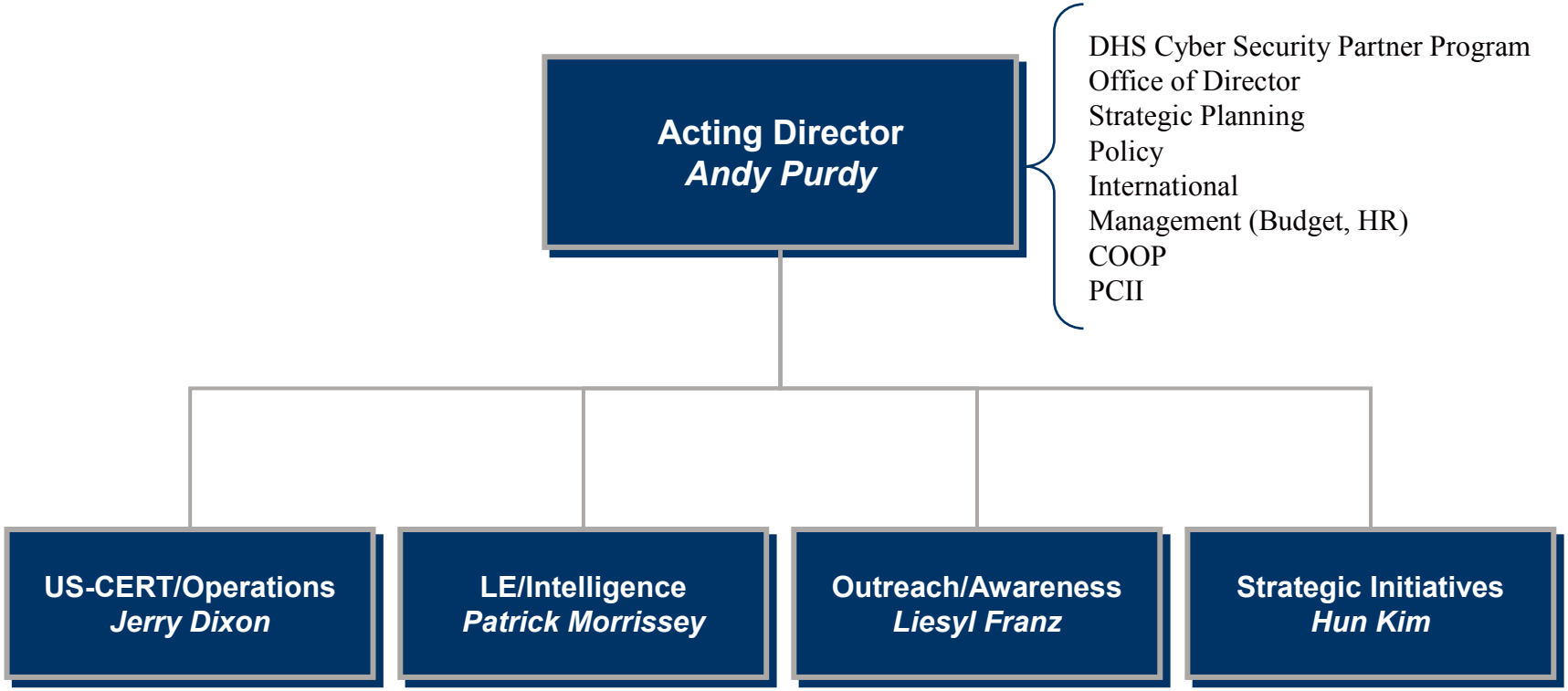
Homeland Security

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



Homeland Security

DHS National Cyber Security Division (NCSD)



Homeland Security

Software Assurance is a NCSD Strategic Initiative

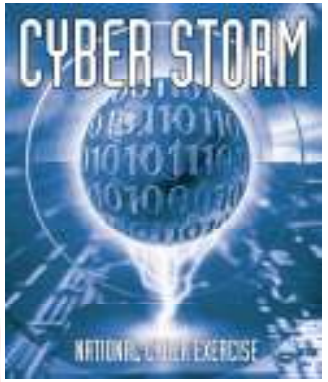
DHS NCSD Priorities:
National Cyber Security Response System

- Watch and Warning
  - Situational awareness
  - 24/7 operations
- Analysis
  - Malicious code
  - Risk analysis
  - LE/Intel
- Response
  - Incident management
- Recovery
  - NRP Cyber Annex
  - ESF-2
  - Regional preparedness

Homeland Security

DHS NCSD Priorities: Cyber Risk Management

- The National Infrastructure Protection Plan (NIPP)
  - Internet Disruption
  - Control Systems
- Outreach and Awareness
- Exercises
  - Regional & International Tabletop exercises
  - TOPOFF and Cyber Storm
  - Future Internet Disruption exercise
- Long Term Planning and Improvement
  - Research and Development
  - Training and Education
  - Standards and Best Practices
- Software Assurance



Homeland Security

Needs in IT/Software Assurance

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

Homeland Security

Strengthen operational resiliency

Shortage of IT/Software workforce with requisite skills

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

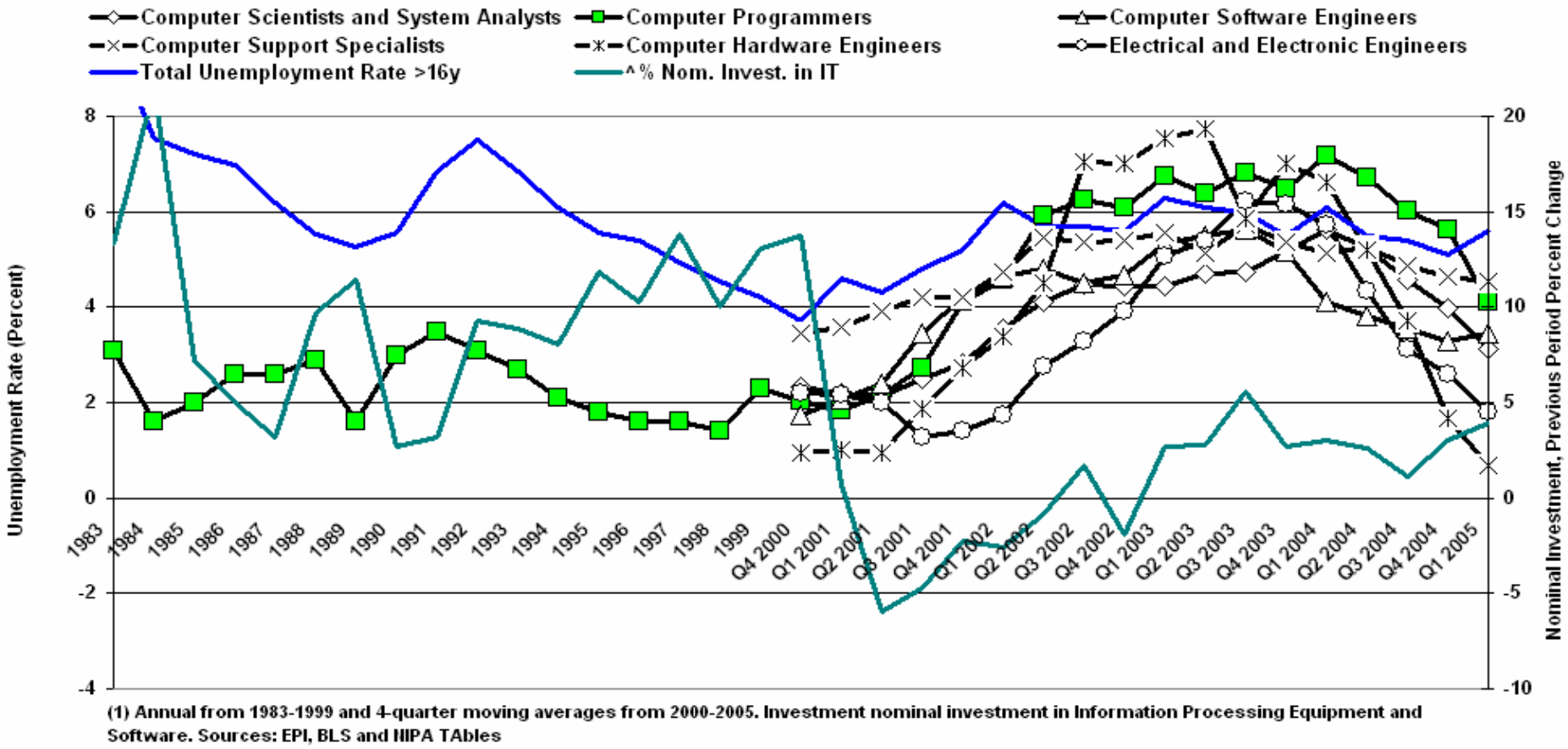
Homeland Security

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

Tech Unemployment & IT Investment:

INSTITUTE FOR INTERNATIONAL ECONOMICS

Total and Select Categories of IT-Related Occupation Unemployment and IT Investment (1)



(1) Annual from 1983-1999 and 4-quarter moving averages from 2000-2005. Investment nominal investment in Information Processing Equipment and Software. Sources: EPI, BLS and NIPA TAbles

Diffusion of IT leads to technology jobs throughout US economy —2/3 of IT workers work outside the IT sector. So, IT professionals exposed to <u>both</u> the tech cycle and business cycle.

Trade, Technology, and Jobs

Cyclical exposure & structural change

INSTITUTE FOR INTERNATIONAL ECONOMICS

US Technology Occupations 1999-End 2004

Occupations	1999	End-2004	Total Change	Percentage Change	Annual Wage 2004	Annual Real Wage Change 1999-2004
Call-Center Type Occupations						
Telemarketers	485,650	407,650	-78,000	-16.1%	$ 23,520	-0.3%
Telephone Operators	50,820	36,760	-14,060	-27.7%	$ 29,980	-0.3%
Low-wage Technology Workers						
Switchboard operators, including answering service	248,570	202,980	-45,590	-18.3%	$ 22,750	0.3%
Computer operators	198,500	133,230	-65,270	-32.9%	$ 33,140	0.8%
Data entry keyers	520,220	307,400	-212,820	-40.9%	$ 24,560	0.6%
Word Processors and Typists	271,310	161,730	-109,580	-40.4%	$ 29,800	1.6%
Desktop Publishers	37,040	30,340	-6,700	-18.1%	$ 34,210	-0.7%
Electrical and electronic equipment assemblers	387,430	207,050	-180,380	-46.6%	$ 27,960	2.5%
Semiconductor processors	42,110	43,420	1,310	3.1%	$ 32,080	0.6%
Total Call-Center and Low-Wage Tech. Workers	**2,241,650**	**1,530,560**	**-711,090**	**-31.7%**	**$ 26,539**	**0.7%**
Comparable; Production Workers in the Manufacturing Sector				**-19%**		
Mid-Level IT Workers						
Computer Support Specialists	462,840	491,680	28,840	6.2%	$ 43,660	-0.5%
High-wage Technology Workers						
Computer and information scientists, research	26,280	26,950	670	2.5%	$ 90,860	3.7%
Computer programmers	*528,600*	*396,100*	*-132,500*	*-25.1%*	*$ 66,480*	*1.3%*
Computer software engineers, applications	287,600	439,720	152,120	52.9%	$ 78,570	1.1%
Computer software engineers, systems software	209,030	321,120	112,090	53.6%	$ 83,460	2.2%
Computer systems analysts	428,210	497,100	68,890	16.1%	$ 69,470	1.2%
Database administrators	101,460	100,420	-1,040	-1.0%	$ 64,380	1.6%
Network and computer systems administrators	204,680	262,930	58,250	28.5%	$ 62,300	1.9%
Network systems and data communications analysts	98,330	176,840	78,510	79.8%	$ 64,080	0.3%
Computer hardware engineers	60,420	79,670	19,250	31.9%	$ 85,540	2.5%
Electrical engineers	149,210	147,120	-2,090	-1.4%	$ 75,540	1.6%
Electronics engineers, except computer	106,830	133,410	26,580	24.9%	$ 78,620	1.8%
Total High-wage Tech. Workers	**2,200,650**	**2,581,380**	**380,730**	**17.3%**	**$ 71,680**	**1.7%**
Comparable; Total CES Employment				**3%**		

Source: Bureau of Labor Statistics CES Data, 1999, 2000, 2001, 2002, May 2003, November 2003 and May 2004 National Occupational Employment and Wage Estimates

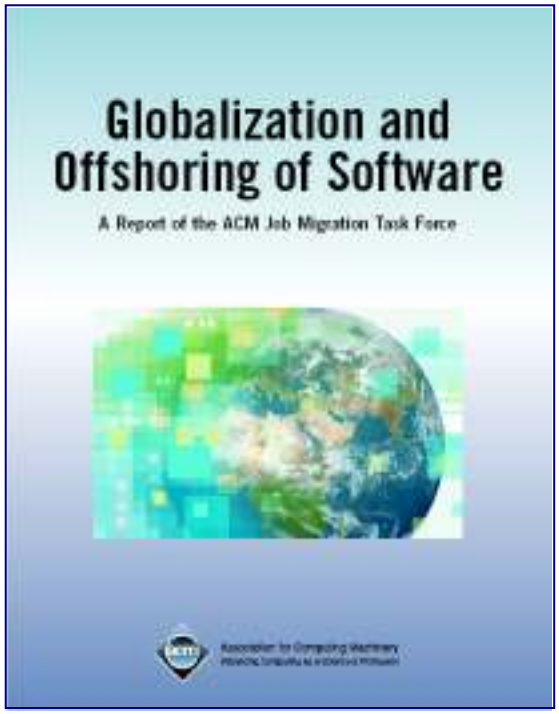
Low-wage in real trouble—from trade & technology

Increased 'codification' puts some high-wage at risk (programming)

Increased jobs at middle & high-wage demand integrative & analytical skills

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

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



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

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

http://www.acm.org/globalizationreport

ACM 2006 "Globalization and Offshoring of Software"
Findings & Recommendations -- Implications for Software Assurance

- **More IT jobs in the US – among the fastest-growing occupations**
  - Data from US Bureau of Labor Statistics (BLS) reports, "despite a significant increase in offshoring over the past five years, more IT jobs are available today in the US than at the height of the dot.com boom."
  - US BLS predicts IT jobs to be "among the fastest-growing occupations over the next decade."
- **Global competition in higher-end skills is increasing -- these trends have implications for individuals, companies, and countries**
  - IT workers & students improve their chances of long-term employment in IT occupations by:
    - obtaining a strong foundational education,
    - learning the technologies used in the global software industry,
    - keeping skills up to date throughout their career,
    - developing good teamwork and communication skills,
    - becoming familiar with other cultures, and
    - managing their careers so as to choose work in industries and jobs occupations less likely to be automated or sent to a low-wage country.
- **Offshoring between developed and developing countries benefit both**
  - Other countries benefit from generating new revenue and creating high-value jobs;
  - US-based corporations achieve better financial performance as a result of the cost savings associated with offshoring some jobs *and* investing increased profits in growing business opportunities that create new jobs in the US.

http://www.acm.org/globalizationreport

ACM 2006 "Globalization and Offshoring of Software"
Findings & Recommendations -- Implications for Software Assurance

- To stay competitive in a global IT environment, countries must adopt policies that foster innovation – educational policy and core investment.
  - To this end, policies that improve a country's ability to attract, educate, and retain the best IT talent are critical.
  - Building a foundation to foster the next generation of innovation and invention requires:
    - Sustaining or strengthening technical training and education systems,
    - Sustaining or increasing investment in research and development, and
    - Establishing governmental policies that eliminate barriers to the free flow of talent.
  - There are some general principles that all countries can follow to mount an effective educational response to offshoring:
    - Evolve computing curriculum at a pace and in a way that better embraces the changing nature of IT.
    - Ensure computing curriculum prepare students for the global economy.
    - Teach students to be innovative and creative.
    - Evolve curriculum to achieve a better balance between foundational knowledge of computing on the one hand, and business and application domain knowledge on the other.
    - Invest to ensure the educational system has good technology, good curriculum, and good teachers.

http://www.acm.org/globalizationreport

ACM 2006 "Globalization and Offshoring of Software"
Findings & Recommendations -- Implications for Software Assurance

- **Offshoring magnifies risks and creates new threats to national security, business property and processes, and individuals' privacy – businesses and nations should employ strategies to mitigate them**
  - When businesses offshore work, they increase not only their own business-related risks they also increase risks to national security and individuals' privacy.
    - intellectual property theft, failures in longer supply chains, or
    - complexity arising from conflicting legal environments
  - Businesses have a clear incentive to manage these new risks to suit their own interests, but nations and individuals often have little awareness of the exposures created.
    - Many nations have COTS software and Internet Protocol technologies in IT-based military systems and critical infrastructure systems.
      - Many COTS systems are developed offshore, making it difficult for buyers to understand source/code.
      - Creates possibility that a hostile nation or non-governmental hostile agents (terrorist/criminal) can compromise these systems.
    - Individuals often are exposed to loss of privacy or identity theft.
      - Bank records, transaction records, call center traffic, and service centers all are being offshored today.
      - Voluminous medical records are being transferred offshore, read by clinicians elsewhere, stored and manipulated in foreign repositories, and managed under much less restrictive laws about privacy and security than in most developed countries.
  - Companies and governments need risk mitigation strategies to address offshoring:
    - Companies should have security and data privacy plans and be certified to meet certain standards;
    - Service providers should not outsource work without the explicit approval of the client;
    - Offshoring providers should be vetted carefully;
    - Businesses should encrypt data transmissions/minimize access to databases by offshore operations;
    - Nations can adopt stronger privacy policies, invest in research methods to secure this data,
    - Nation-to-nation & international treatment of data and how compromises will be handled is needed.

Offshoring also sought due to shortage of IT students & workforce in US

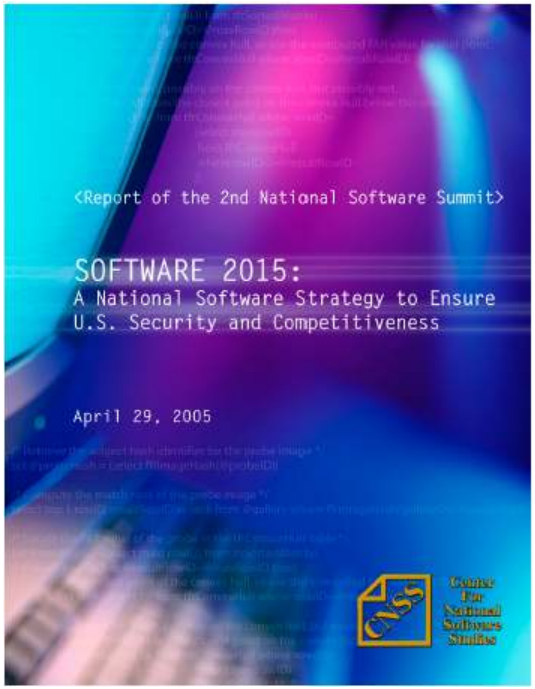
- **Current shortage of IT/software professionals in the US and enrollment declines in relevant disciplines partially driven by misperceptions**
- **Offshore sources sometimes sought to fill void of qualified US IT workforce**
- **Schools must provide relevant curriculum for students to be competitive in a global IT economy; focus needed on requisite core competencies in IT/software**
  - Computer programming easily offshored;
  - Domestic demand is high in IT/computing & information research, software engineering, systems analysts, network and systems administration, network and data communications analysts;
  - Domestic demand raising in all aspects of cyber security and information assurance; increasing needs associated with software assurance.
- **To stay competitive in global IT environment, a US national focus is needed to reverse trends to increase enrollments in IT/computing disciplines**
  - Improvement needed in state-of-the-practice and state-of-the-art for IT/SW capabilities
  - Computing curriculum needs to embrace changing nature of IT/software business
  - Educational policy and investment needed to foster innovation and increase IT-related enrollments

Homeland Security

United States 2nd National Software Summit

Report, **"Software 2015: a National Software Strategy to Ensure US Security and Competitiveness"** 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 using public-private partnerships involving government, industry and academia
- **National Software Strategy** -- four major programs
  - **Improving Software Trustworthiness**
  - **Educating and Fielding the Software Workforce**
  - **Re-Energizing Software Research and Development**
  - **Encouraging Innovation Within U.S. Software Industry**

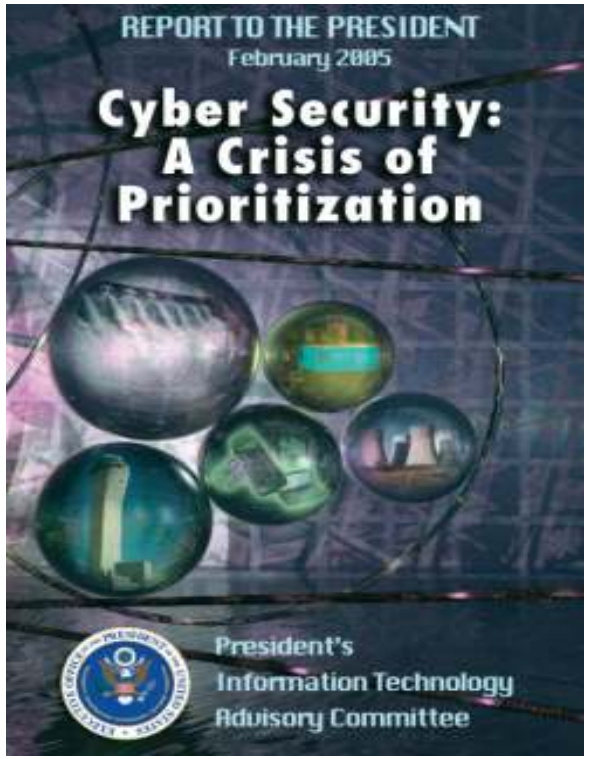


➢ Purpose of National Software Strategy:
- Achieve ability to routinely develop and deploy trustworthy software products
- Ensure the continued competitiveness of the US software industry

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

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

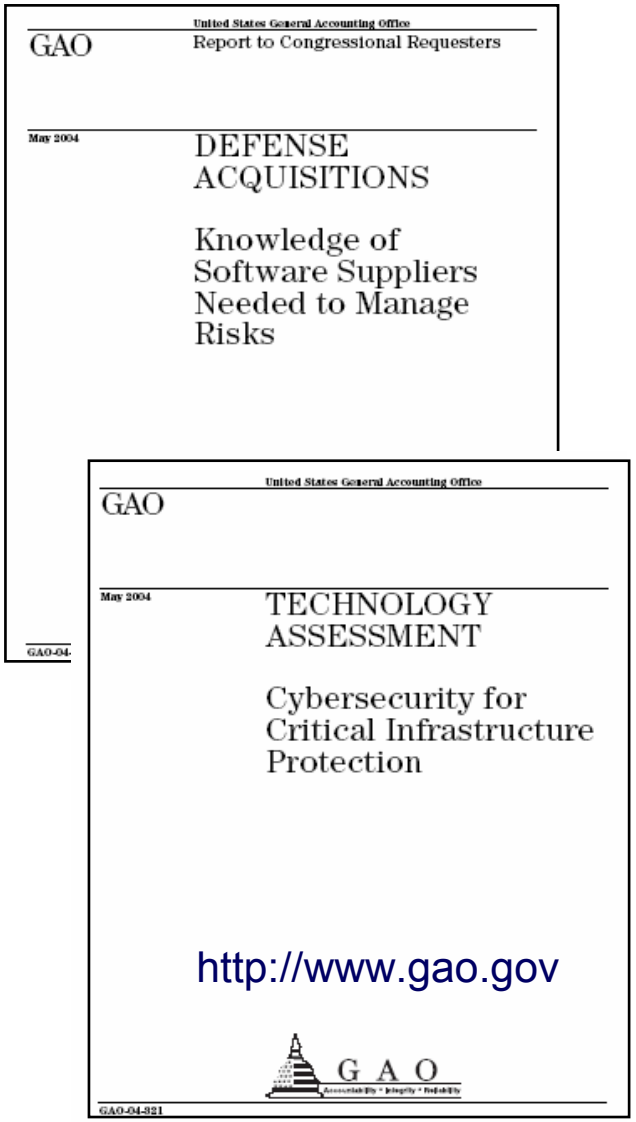
- Commercial software engineering today lacks the scientific underpinnings and rigorous controls needed to produce high-quality, secure products at acceptable cost.
- Commonly used software engineering practices permit dangerous errors, such as improper handling of buffer overflows, which enable hundreds 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.
- **Recommendations for increasing investment in cyber security provided to NITRD Interagency Working Group for Cyber Security & Information Assurance R&D**



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

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
  - 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-06-392 Report, **"Information Assurance: National IA Partnership Offers Benefits, but Faces Considerable Challenges,"** March 2006



Why Software Assurance is Critical

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

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

Homeland Security

Knowledge of Supply Chain & Software Content

- Transparency of the Supply Chain should be an important element of an organization's Risk Management efforts.
- Supplier identity and software content often blurred by reuse of legacy code, sub-contracting, outsourcing and use of open source software (OSS).
- OSS represents a major perturbation in software development processes, in software distribution and acquisition, and in the lifecycle aspects of usage.
  - OSS code is everywhere -- it will find its way into organizations in many ways,
  - IT environments will be comprised of "mixed code"
- Tools needed to deliver transparency of supply chain and software content, (ie., the identification of software elements, combined with increasingly rich information about the identified software elements).
- Transparency of software content ultimately translates into increased security of IT operations, and is a new weapon in the mission to secure cyberspace, and maintain more resilient critical infrastructure assets.

Homeland Security

http://www.gao.gov

What has Caused Software Assurance Problem

Increasing software vulnerabilities and exploitation

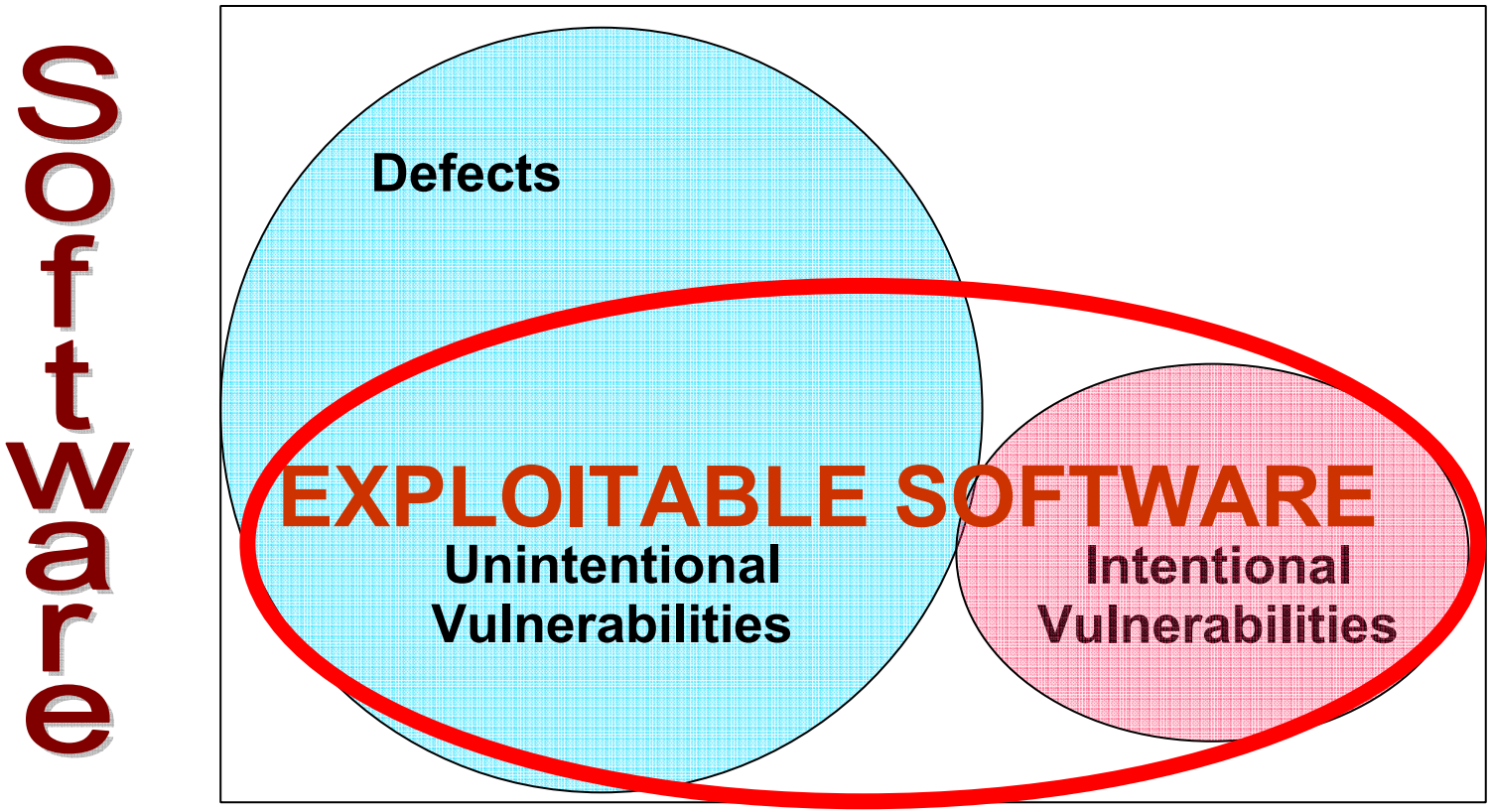
- Then
  - Domestic dominated market
  - Stand alone systems
  - Software small and simple
  - Software small part of functionality
  - Custom and closed development processes (cleared personnel)
  - Adversaries known, few, and technologically less sophisticated
- Now
  - Global market
  - Globally network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

Homeland Security

Software Assurance Addresses Exploitable Software:

Outcomes of non-secure practices and/or malicious intent

Exploitation potential of vulnerability is independent of "intent"



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

Homeland Security

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

“Software Assurance”

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

Software Assurance (SwA) is: “the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner” — Source: Committee on National Security Systems (CNSS) Instruction No. 4009, “National Information Assurance Glossary”, Revised 2006 — http://www.cnss.gov/instructions.html

Alternate definitions:

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

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

Software Assurance (SwA) is scoped to address:

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

Software Assurance is a strategic initiative of the U.S. Department of Homeland Security to promote integrity, security, and reliability in software. The Program is based upon the National Strategy to Secure Cyberspace - Action/Recommendation 2-14: “DHS will facilitate a national public-private effort to promulgate best practices and methodologies that promote integrity, security, and reliability in software code development, including processes and procedures that diminish the possibilities of erroneous code, malicious code, or trap doors that could be introduced during development.” DHS SwA "Build Security In" Portal

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

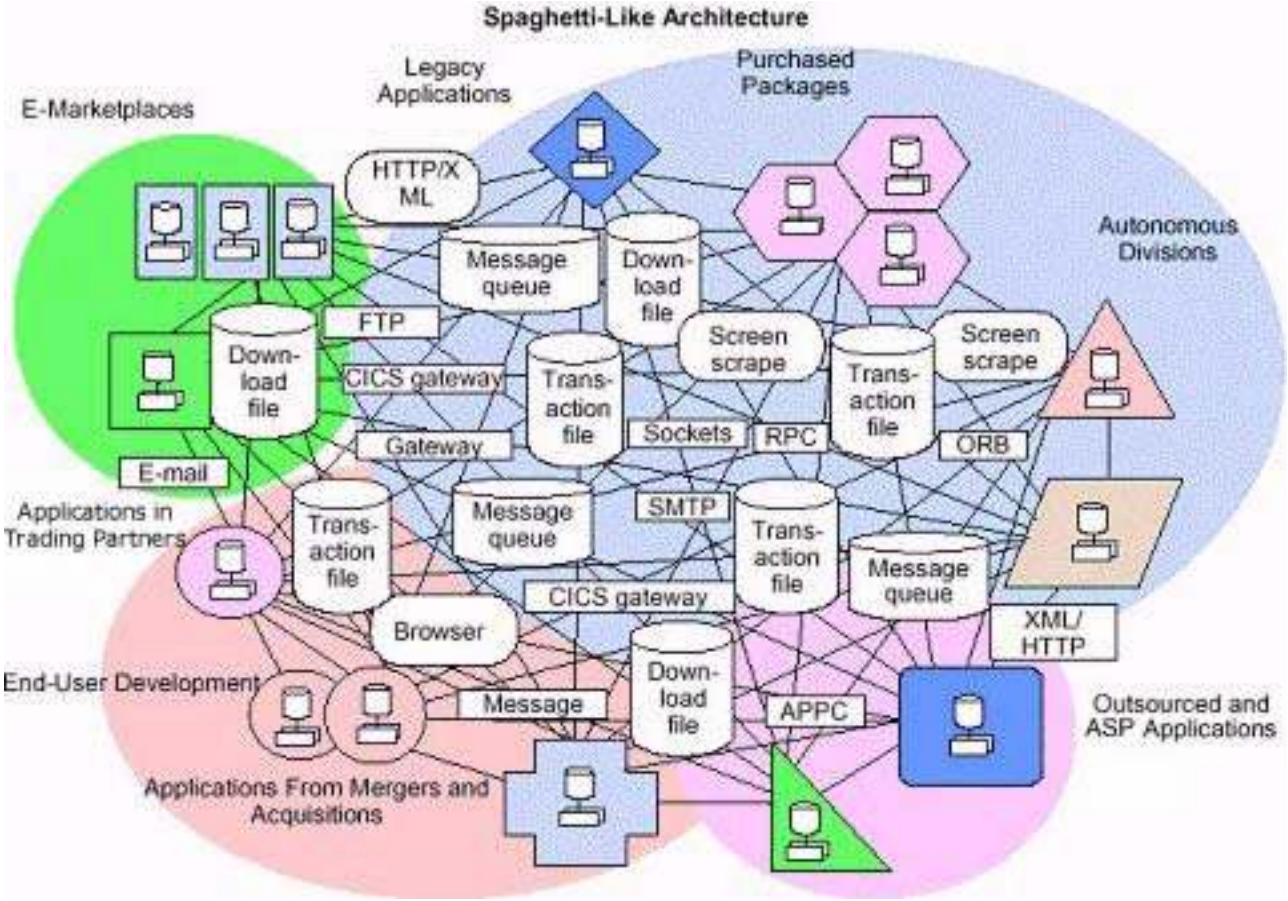
Homeland Security

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.

Homeland Security

Reality of Existing Software



complex, multiple technologies with multiple suppliers

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

Homeland Security

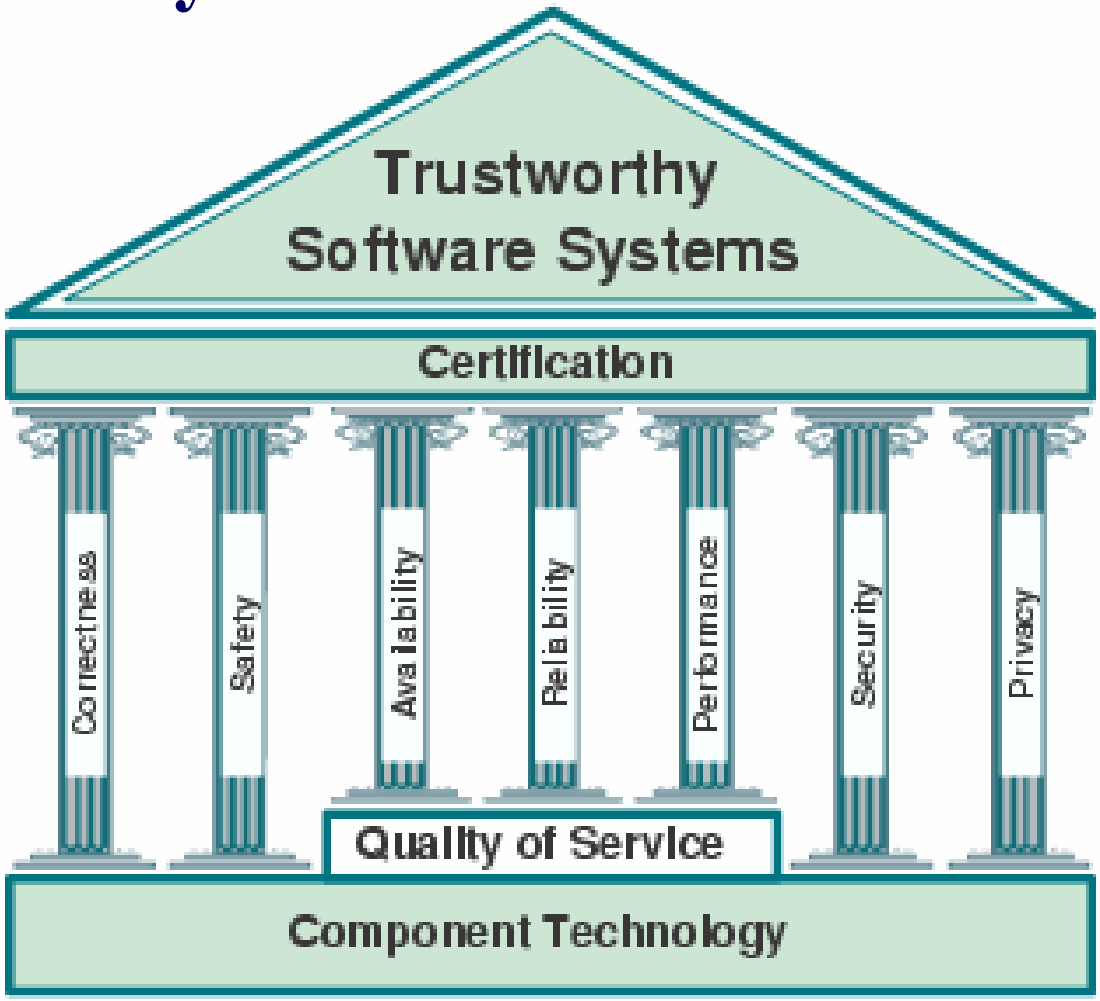
Gartner

Software Assurance contributes to Trustworthy Software Systems

Suppliers must consider enabling technologies and lifecycle processes

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

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



Homeland Security

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

Software Assurance Comes From:

Knowing what it takes to "get" what we want

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

Building and/or acquiring what we want

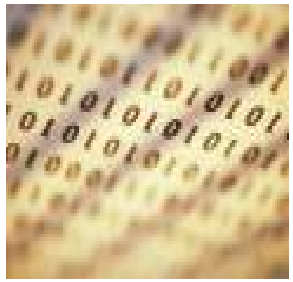
- Threat modeling and analysis
- Requirements engineering
- Failsafe design and defect-free code
- Supply Chain Management

Understanding what we built / acquired

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

*Multiple Sources:

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



Using what we understand

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

Homeland Security

Software Assurance Lifecycle Considerations

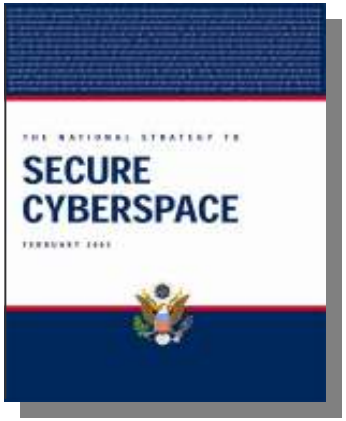
- Define Lifecycle Threats/Hazards, Vulnerabilities & Risks
- Identify Risks attributable to software
- Determine Threats (and Hazards)
- Understand key aspects of Vulnerabilities
- Consider Implications in Lifecycle Phases:
  - Threats to: System, Production process, Using system
  - Vulnerabilities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

Homeland Security

DHS Software Assurance Program Overview

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

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



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

Homeland Security

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

DHS Software Assurance Program Structure

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

Homeland Security

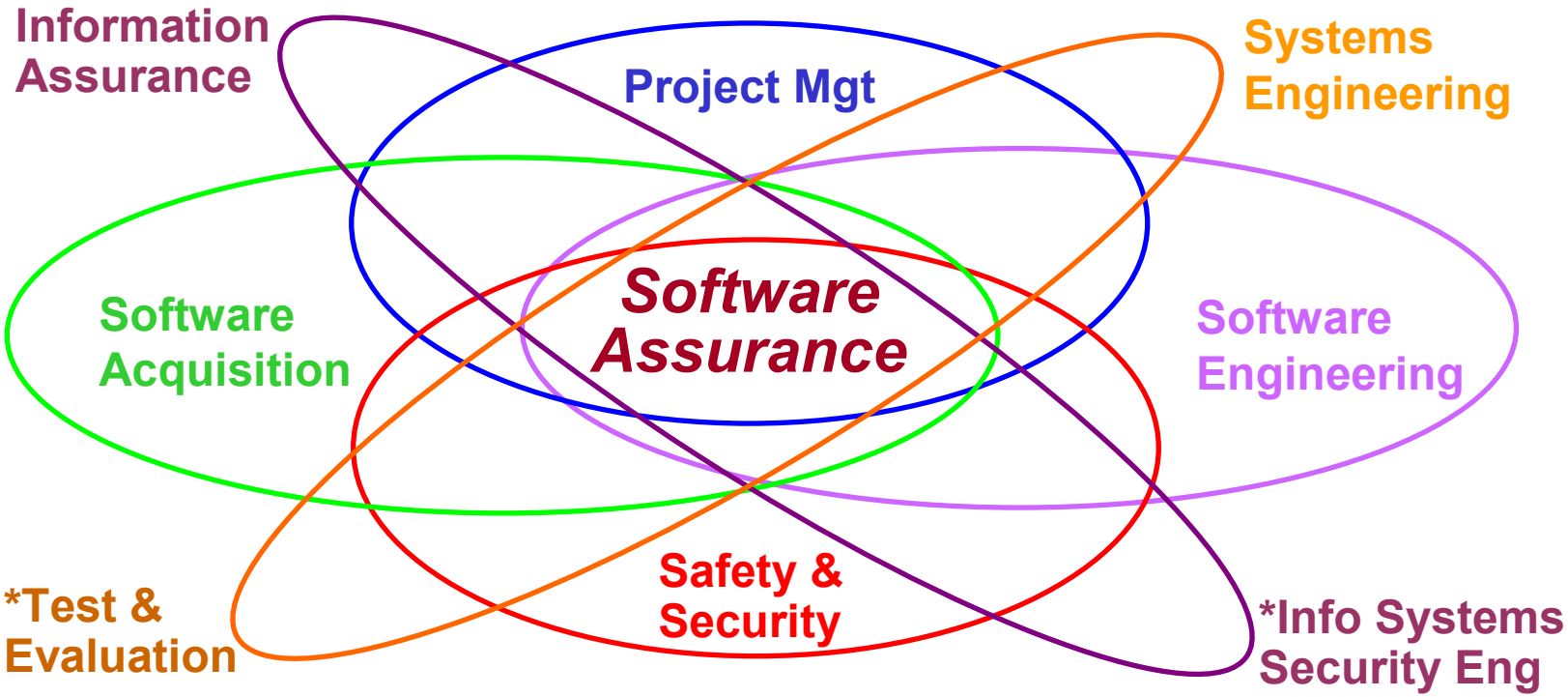
DHS Software Assurance: People

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

Homeland Security

**NCSD Objective/Action 1.4.1

Disciplines Contributing to SwA CBK*



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

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

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

Homeland Security

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

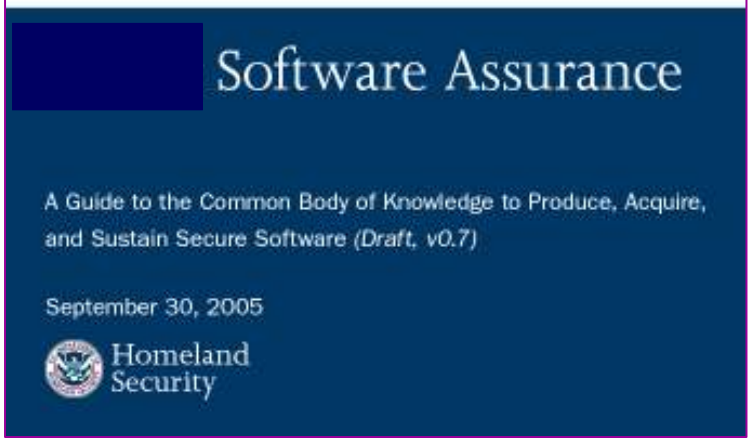
The intent is not to create a new profession of Software Assurance; rather, to provide a common body of knowledge: (1) from which to provide input for developing curriculum in related fields of study and (2) for evolving the contributing disciplines to better address the needs of software security, safety,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

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

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

Information for Educators & Trainers

(version 1.0 released May 2006)



Initial focus on "Secure Software"

Homeland Security

Software Assurance Common Body of Knowledge

General Changes throughout Document

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

Homeland Security

Software Assurance Common Body of Knowledge

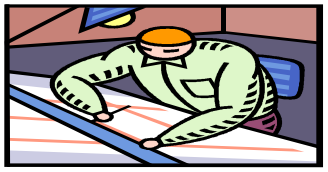
- **Changes to "Threats and Hazards" Section**
  - Focus on role vulnerable software plays in enabling exploits against *data*
  - Attack examples added from sectors other than National Security
  - Individual attack patterns descriptions replaced attack categories pointing to recognized sources of private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

Reaching Relevant Stakeholders

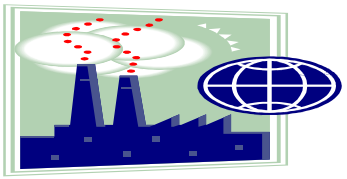
Leverage Evolving Efforts in Universities, Standards Organizations & Industry

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

University acceptance



Individual acceptance

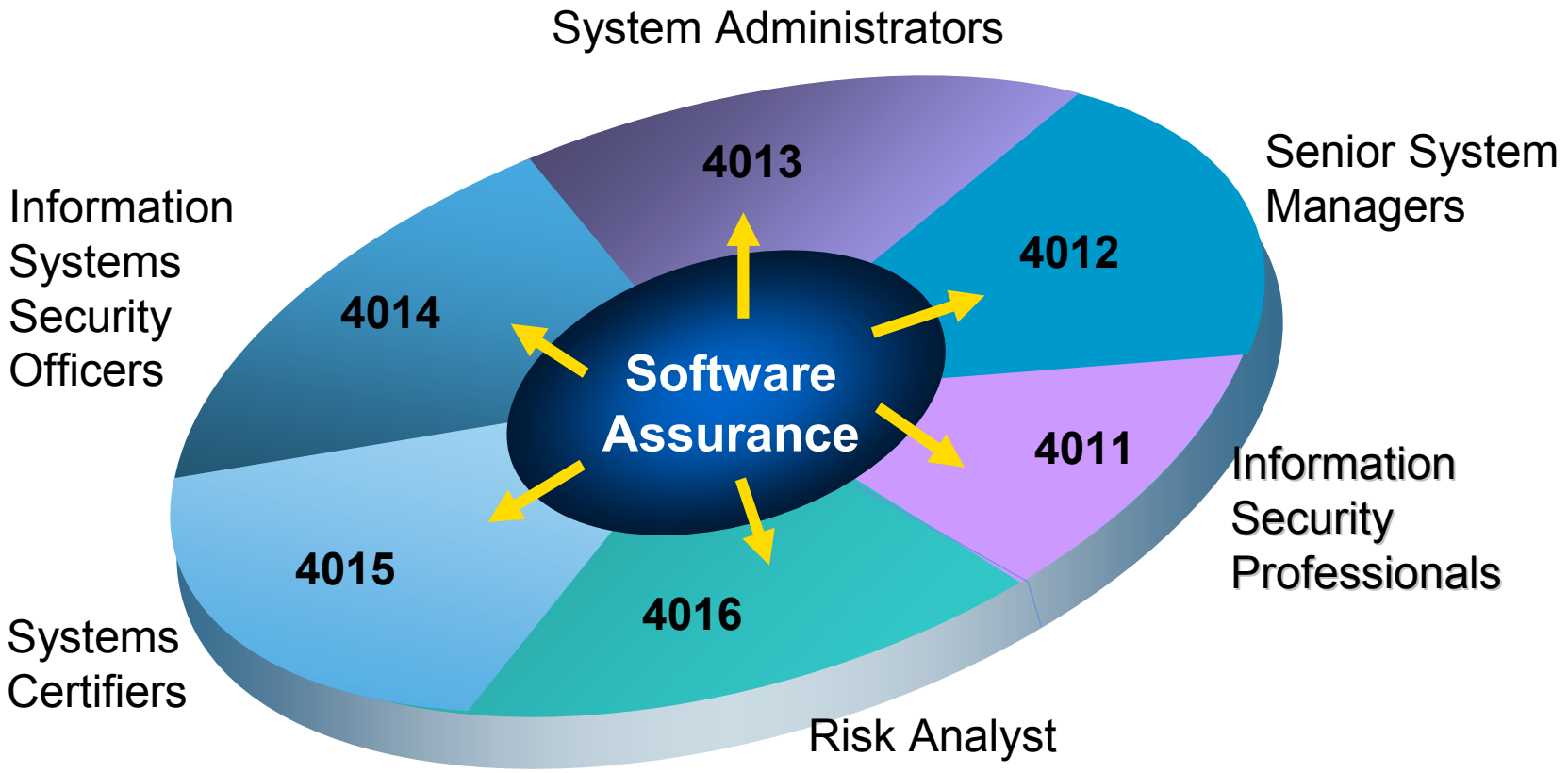


Industry acceptance

Homeland Security

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

Integrating SwA CBK with CNSS IA Standards
(An example path for inserting SwA in Education Curriculum)



Software Assurance considerations for IA functional roles:

-- add SwA material in applicable CNSS 4000 series standards

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

Significance of SwA Education Curriculum

- **Courseware** –
  - Through DoD & DHS co-sponsorship, the Committee on National Security Systems (CNSS) and the National Security Agency (NSA) provide certification that academic institutions offer a set of courseware that has been reviewed by National Level Information Assurance Subject Matter Experts who determine if the institutions meet National Training Standards for Information Systems Security Professionals,
  - NSTISSI No. 4011 for Information Security Professionals (as a minimum, plus at least one of the other 4000 series standards) for specific academic years.

- **Center of Academic Excellence in Information Assurance Education**
  - Designation as CAEIAE by NSA (based on CNSS certification of courseware).
  - See http://www.nsa.gov/ia/academia/caeCriteria.cfm

- **Scholarship for Service (SFS)**
  - **CAEIAE certification** (or qualified equivalent criteria determined by NSA & DHS) is a qualifying requirement for institutions to offer the National Science Foundation (NSF) SFS program.
  - **NSF Federal Cyber Service SFS Federal Cyber Service** Training and Education Initiative at http://www.nsf.gov/pubs/2006/nsf06507/nsf06507.htm
    - **Scholarship Track** -- increase the number of qualified students entering the fields of information assurance and computer security and
    - **Capacity Building** -- increase the capacity of the U.S. higher education enterprise to continue to produce professionals in these fields to meet the needs of our increasingly technological society.

Homeland Security

SwA CBK relative to Computing Curricula

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

Computing Curricula 2005

The Overview Report

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

A volume of the *Computing Curricula Series*

The Joint Task Force for Computing Curricula 2005

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

30 September 2005

Homeland Security

Integrating SwA CBK with IT Security Training
(An example path for inserting SwA in IT Workforce Training Programs)

- Provide input to the DHS-led federal IT workforce training initiative by leveraging evolving efforts in federal government:
  - DoD IA Workforce Training and Certification Requirements for IA Workforce (see DoD 8570.1M)
  - NIST IT Security Training Requirements (see NIST Special Pub 800-16)
  - Federal CIO IT Workforce Council
- Provide recommended core competencies and course content for federal acquisition managers to consider SwA due-diligence in procurement efforts
  - Federal Acquisition Institute (FAI)
  - Defense Acquisition University (DAU)
  - National Defense University Information Resource Management College

Homeland Security

How CAEs advance Software Assurance

- Contribute to SwA Common Body of Knowledge
  - Provide review and constructive feedback
  - Contribute content and add references
  - Provide examples from all spectra of society that highlight the need and motivations for software security
  - Provide content for extending SwA CBK to better address other “ilities”
- Contribute to efforts extending SwA course offerings
  - Provide mappings to related curricula
  - Provide sample course material
  - Provide “lessons learned” in developing and offering courses, including the integration of SwA content in existing courses.

Homeland Security

DHS Software Assurance: Process

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

Homeland Security

**NCSD Goal/Action 1.4.2

DHS Software Assurance: Process (cont.)

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

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

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

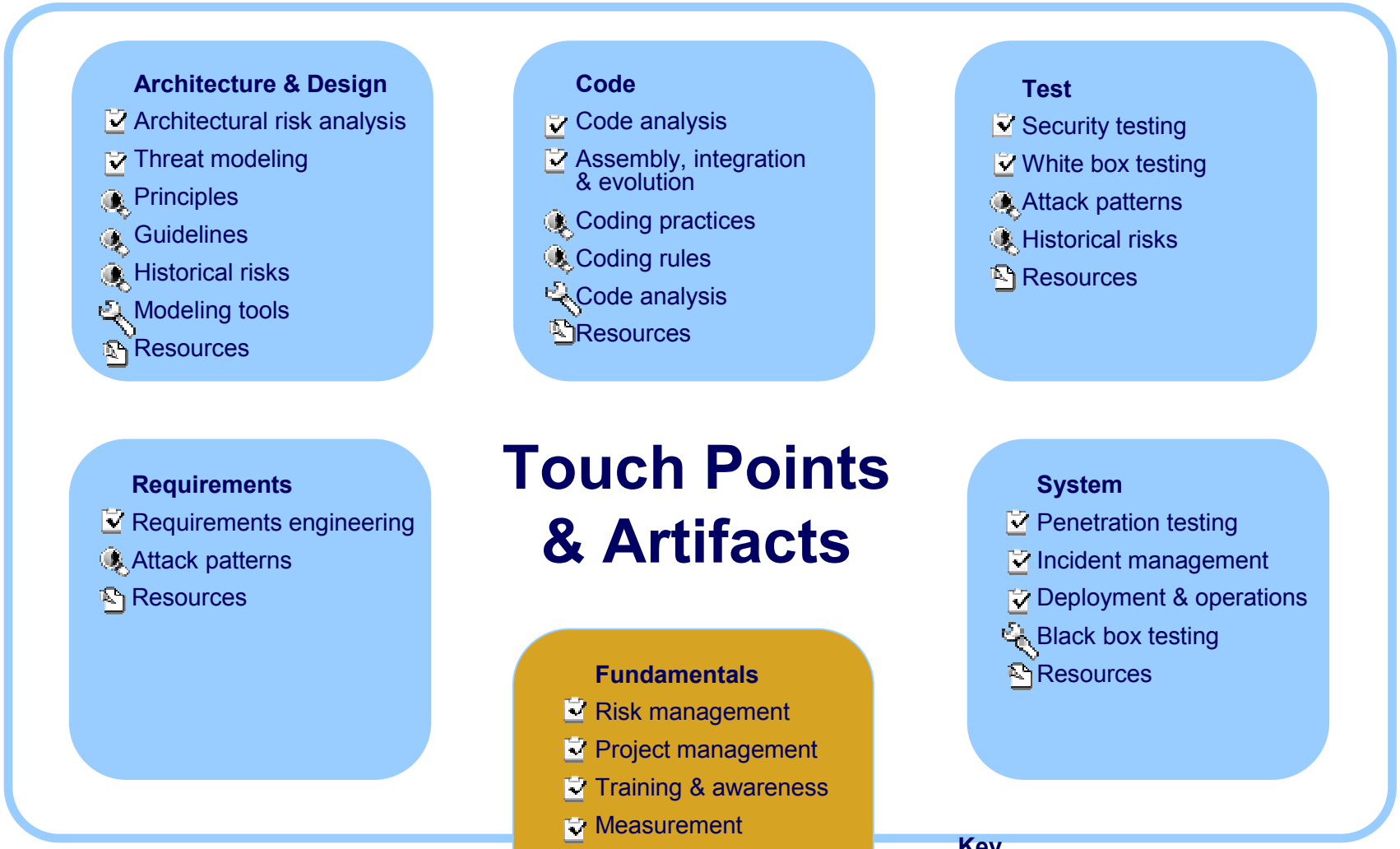
  - Updating site to include additional development guidance and add new focus for acquisition and ops/sustainment

Homeland Security

**NCSD Objective/Action 1.4.2

Process Agnostic Lifecycle

Launched 3 Oct 2005



https://buildsecurityin.us-cert.gov

Homeland Security

DHS Software Assurance: Process (cont.)

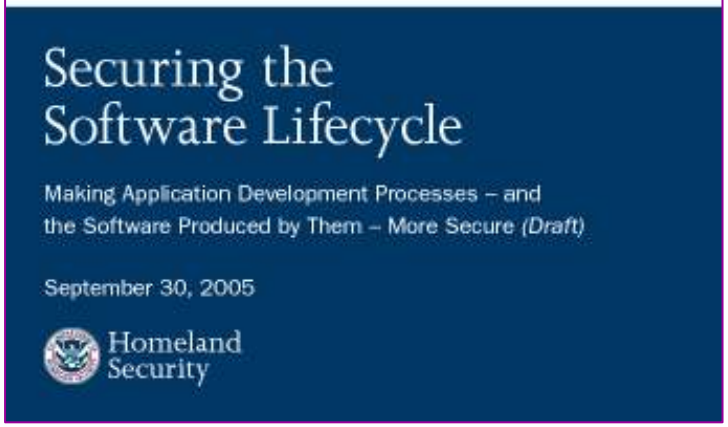
- Provide practical guidance in software assurance practices and process improvement methodologies** (cont.)
  - Released draft developers' guide "SECURING THE SOFTWARE LIFECYCLE: Making Application Development Processes – and Software Produced by Them – More Secure"

• 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

(version 1.0 released April 2006)



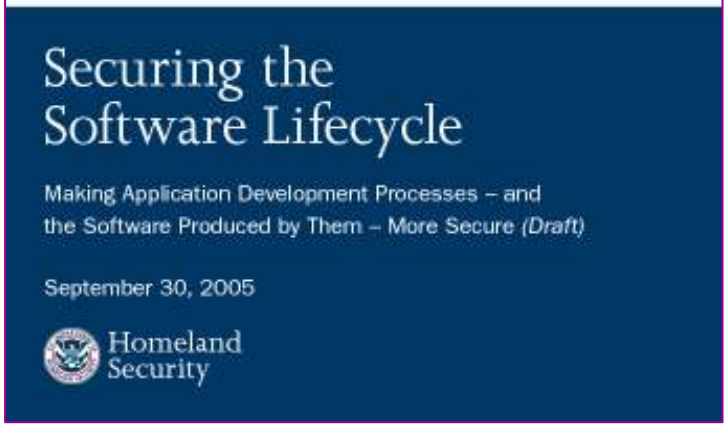
Homeland Security

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

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

Information for Developers

(version 1.0 released April 2006)



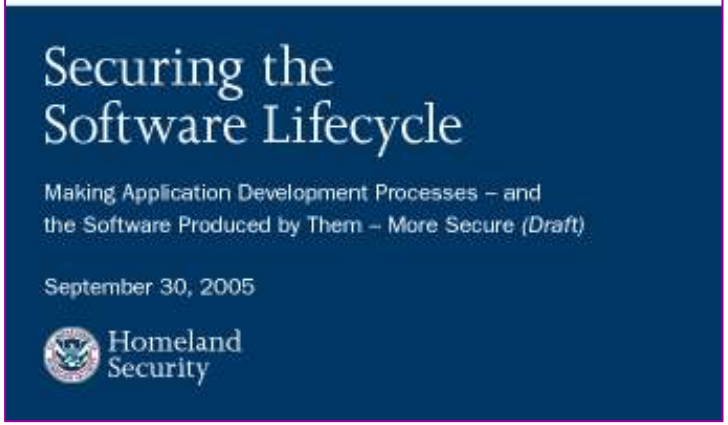
Homeland Security

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

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

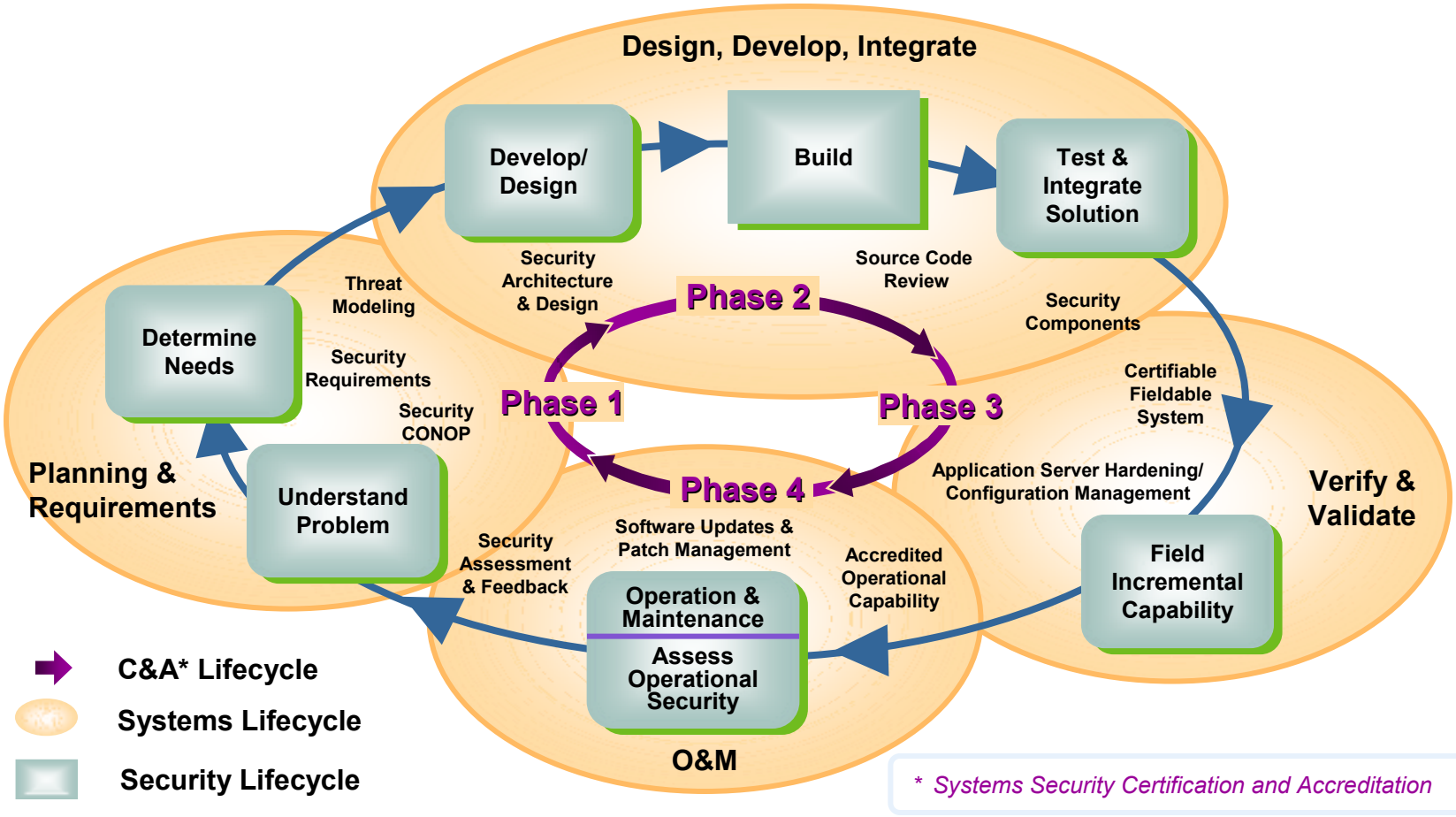
Information for Developers

(version 1.0 released April 2006)



Homeland Security

Integrating security into the systems engineering lifecycle enables software assurance implementation



Homeland Security

Booz | Allen | Hamilton

DHS Software Assurance: Process (cont.)

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

Homeland Security

**NCSD Objective/Action 1.4.2

Value of Standards

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

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

Role of Standards for Software Assurance

- Standards are needed to better enable exchange of information among participants and enable interoperability between solutions (provided by multiple vendors) needed to perform SwA activities.
  - Offer common ground for communication
  - Provide consensus-based, sound practices for engineering
  - Provide benchmarking criteria for gauging the achievement of objectives
  - 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
- Standards relevant to Software Assurance would:
  - Increase interoperability among tools and manual processes by creating an open framework.
  - Provide guidance and criteria for making claims about the integrity (safety, security, & dependability) of products and systems.
  - Enable generation of new solutions to benefit all sectors (Government, Industry, etc)
  - Better ensure that all sectors are investing within a coordinated strategy.

Homeland Security

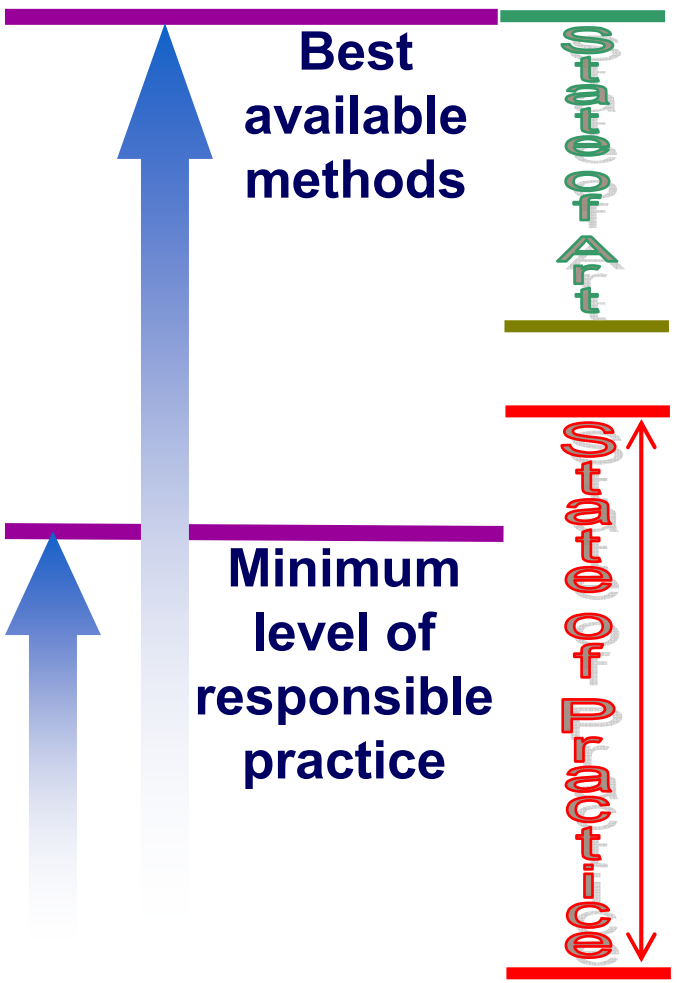
Using Standards and Best Practices to Close gaps between state-of-the-practice and state-of-the-art *1, 2

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

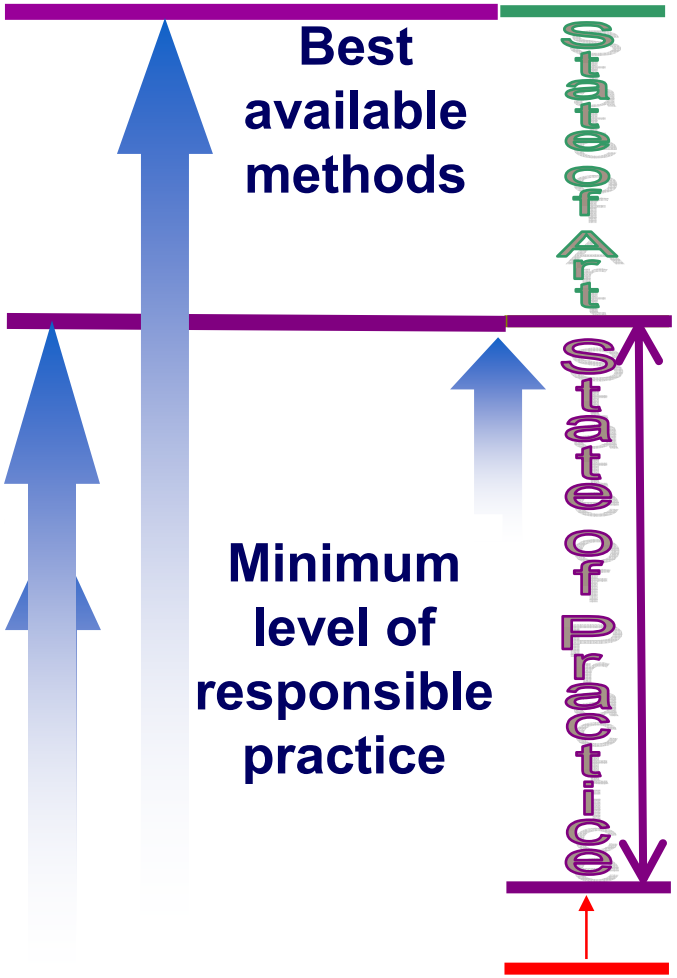
Using Standards and Best Practices to Close gaps between state-of-the-practice and state-of-the-art *1, 2

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.

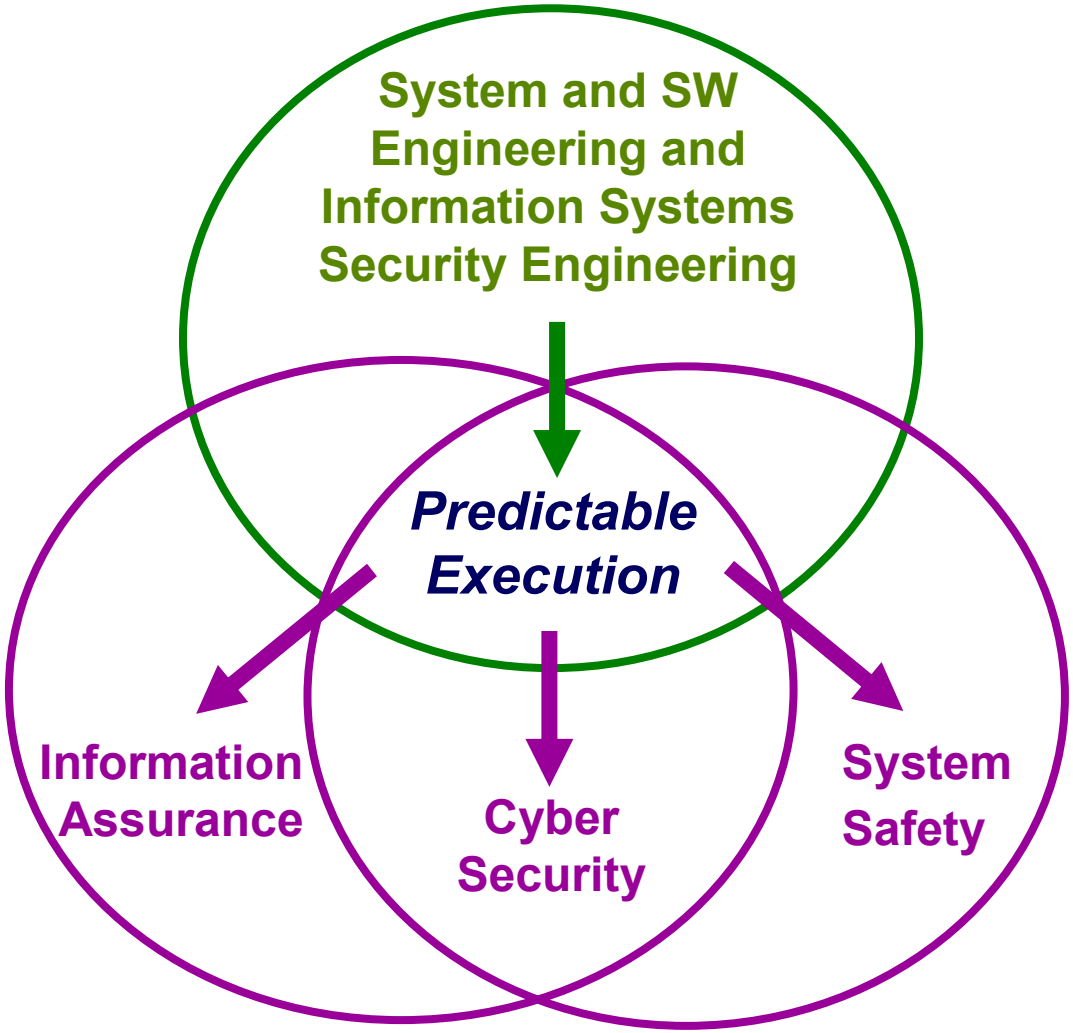
Raising the Floor

- 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



For a safety/security analysis to be valid …

The execution of the system must be *predictable*.

This requires …

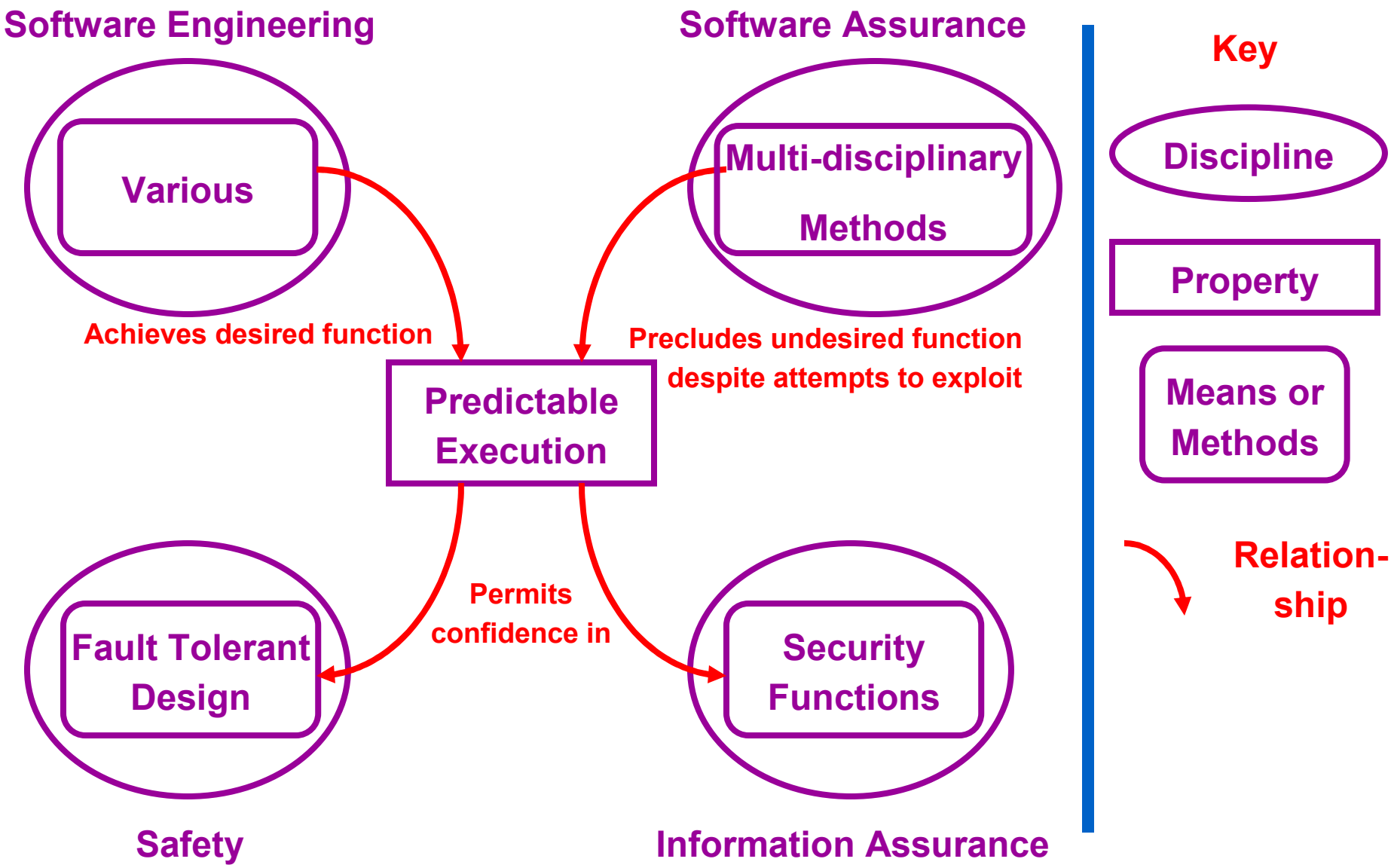
- **Correct implementation of requirements, expectations and regulations.** } ***Traditional concern***
- **Exclusion of unwanted function even in the face of attempted exploitation.** } ***Growing concern***

Homeland Security

Predictable Execution = requisite enabling characteristic

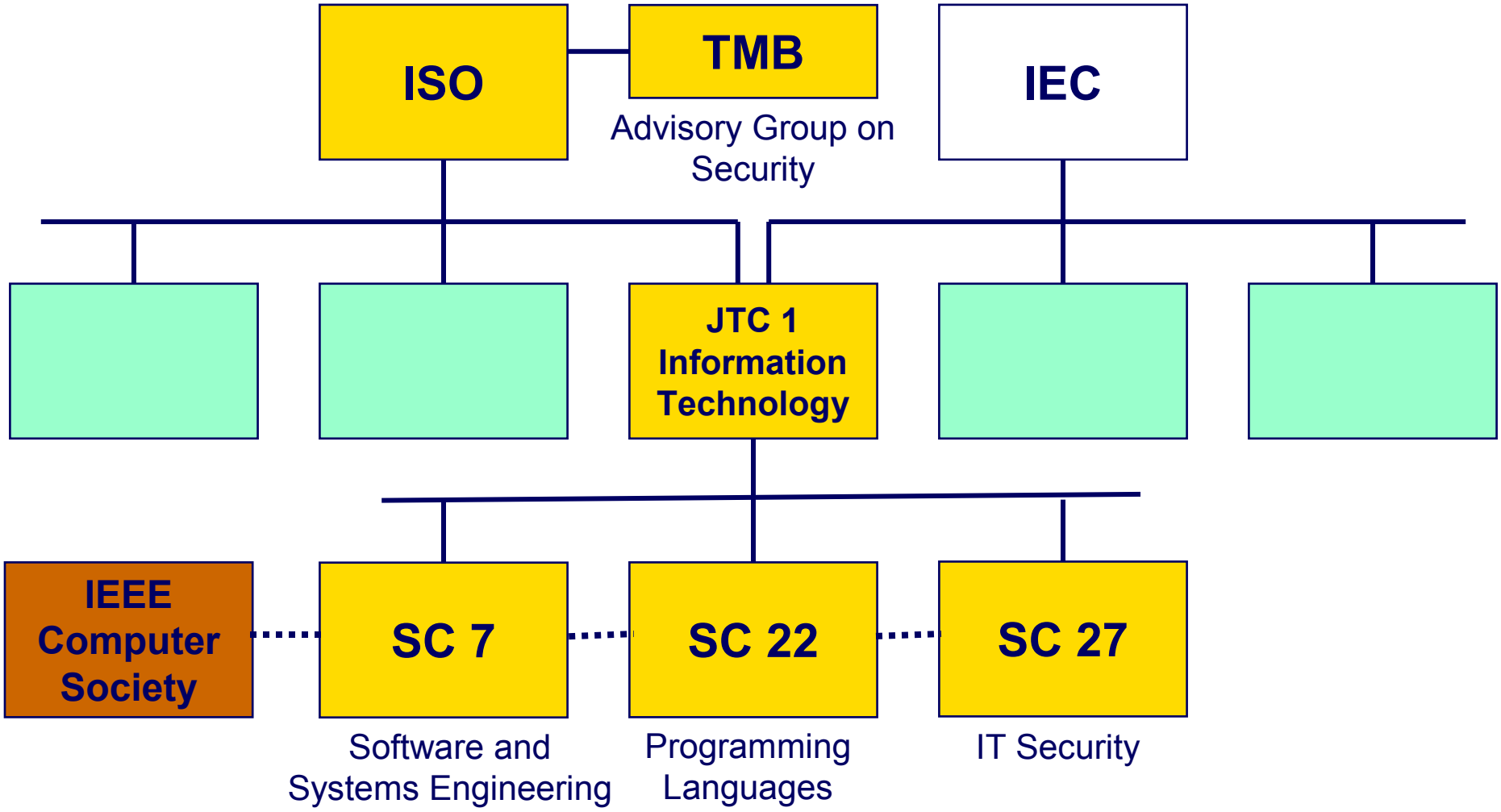
*Adopted from Jim Moore, IEEE CS S2ESC Liaison to ISO SC7

Simplified Relationships among Disciplines



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

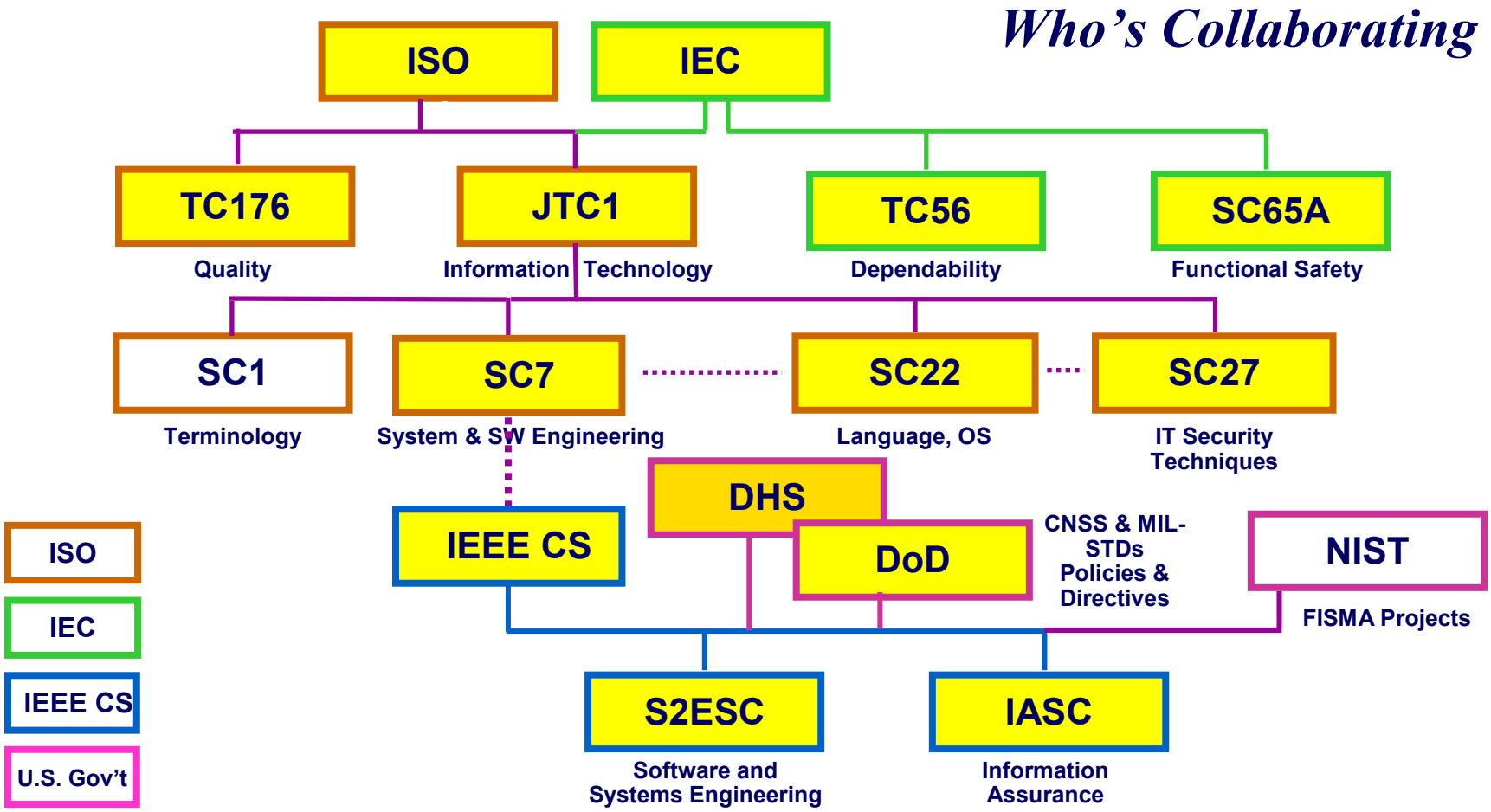
Security and Assurance Concerns in ISO



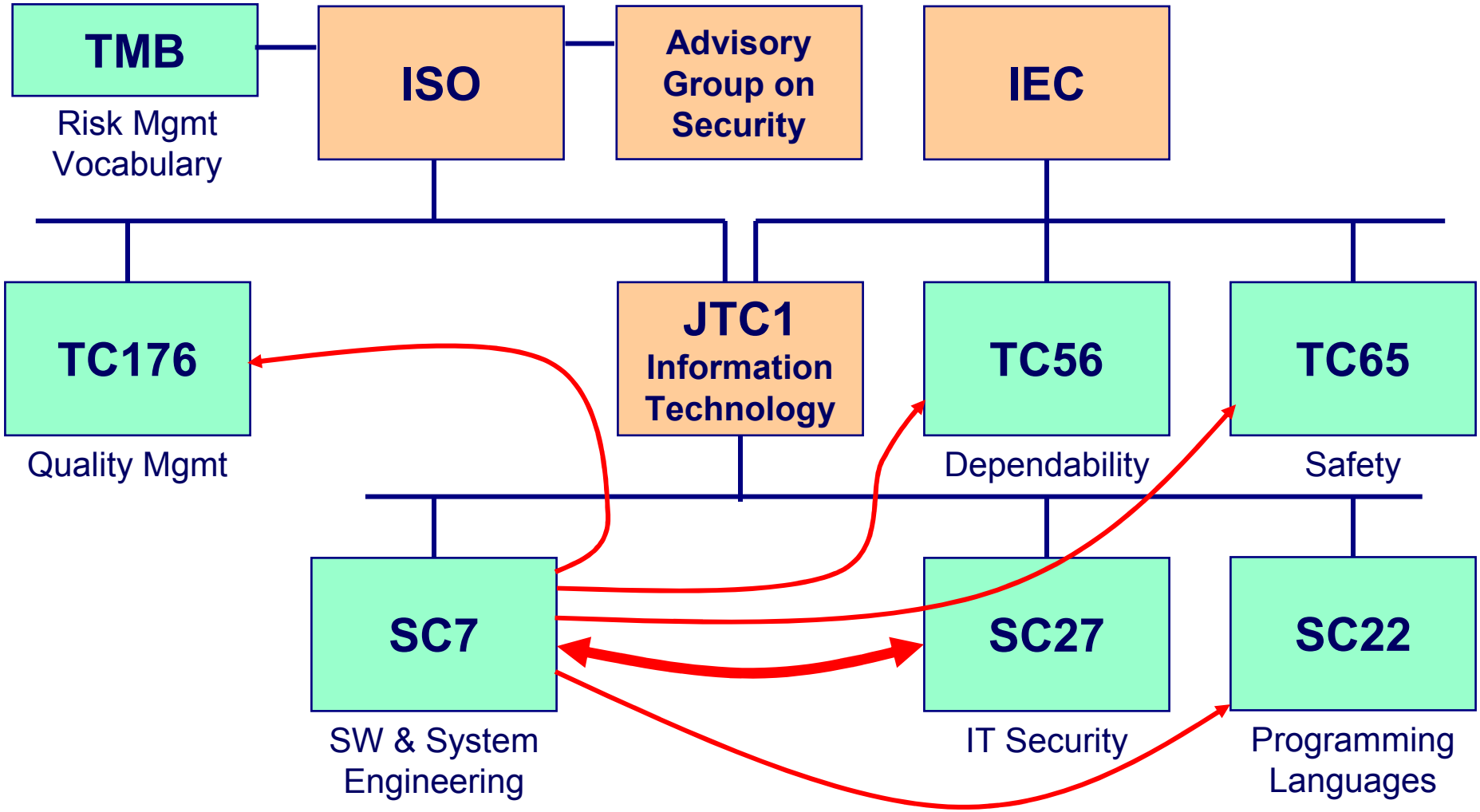
Homeland Security

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

Harmonization Efforts Impacting Systems and Software Assurance



SwA Concerns of Standards Organizations



Homeland Security

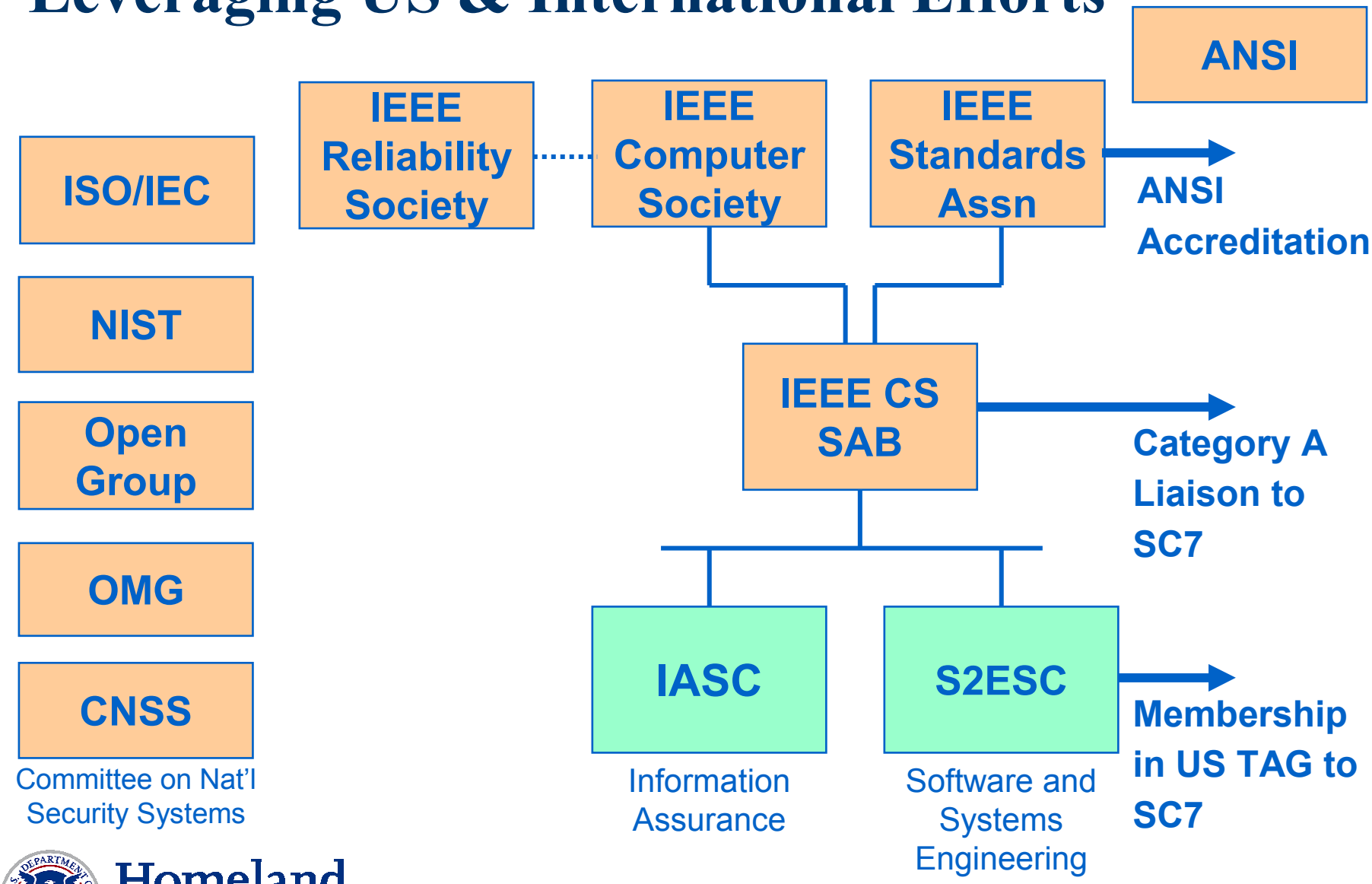
* DHS NCSD has membership on SC7, SC27 & IEEE S2ESC leveraging Liaisons in place or requested with other committees

ISO SC27 (INCITS CS1) Standards Portfolio

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

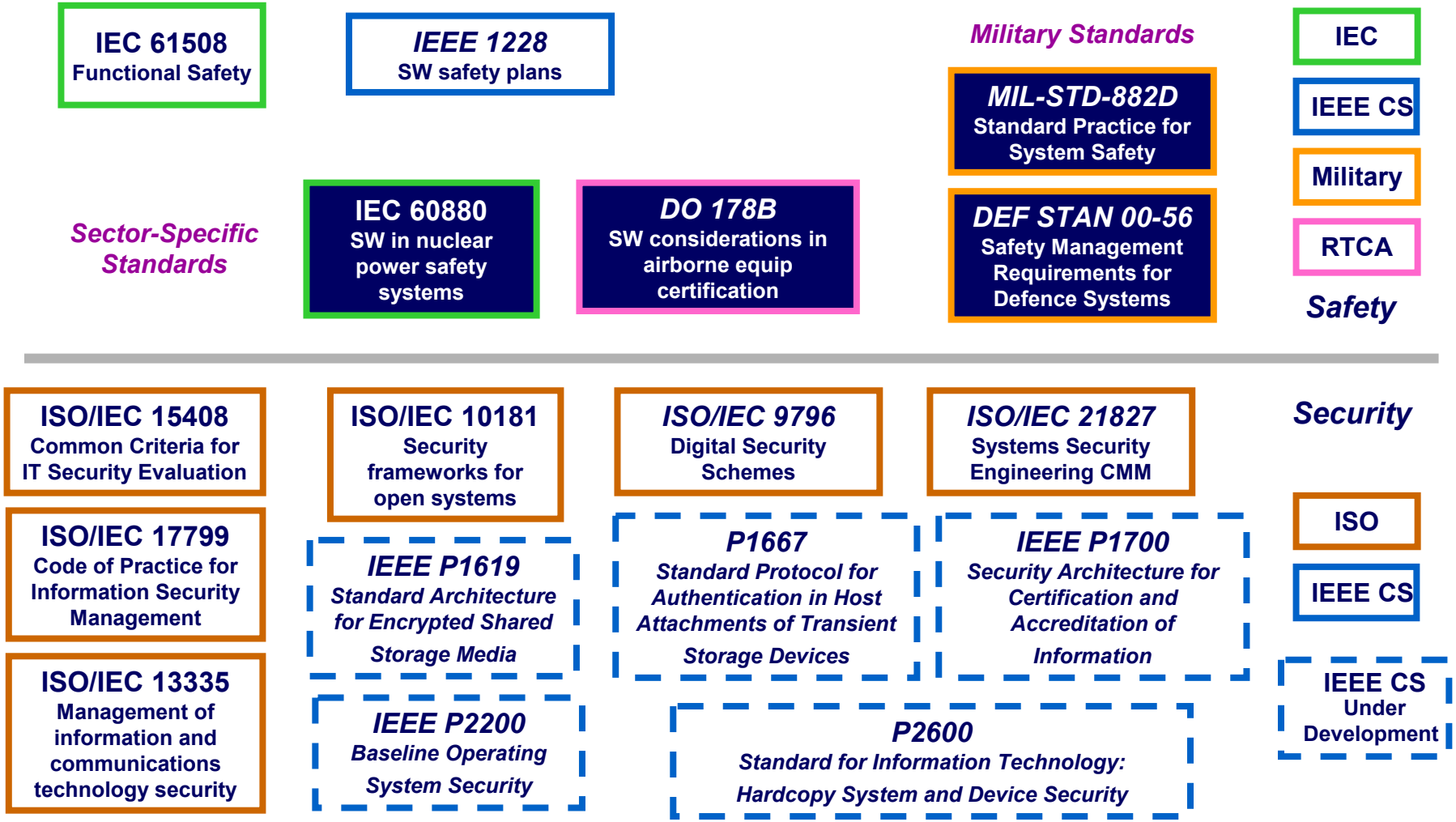
Homeland Security

Leveraging US & International Efforts



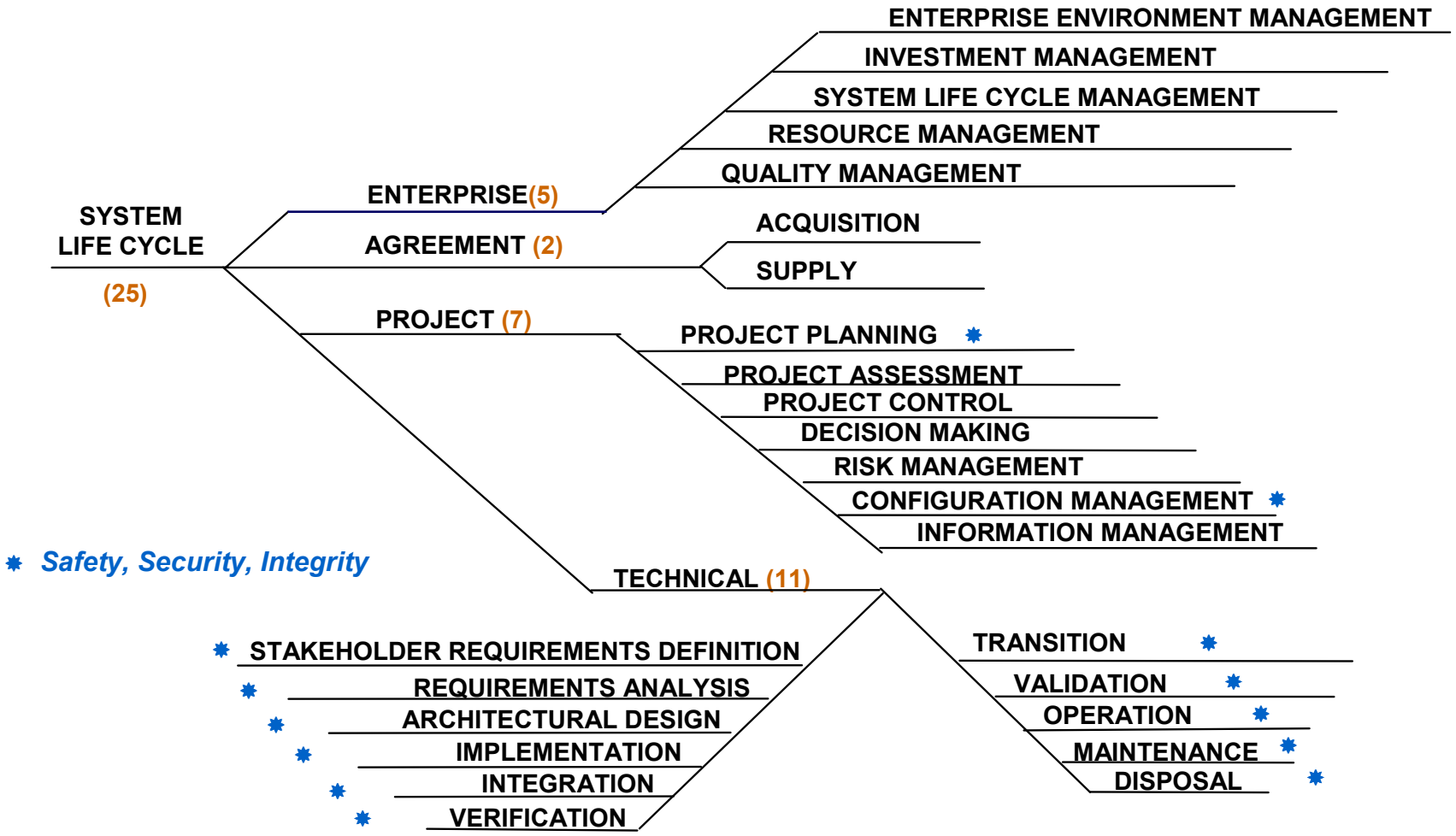
Homeland Security

Safety and Security Standards



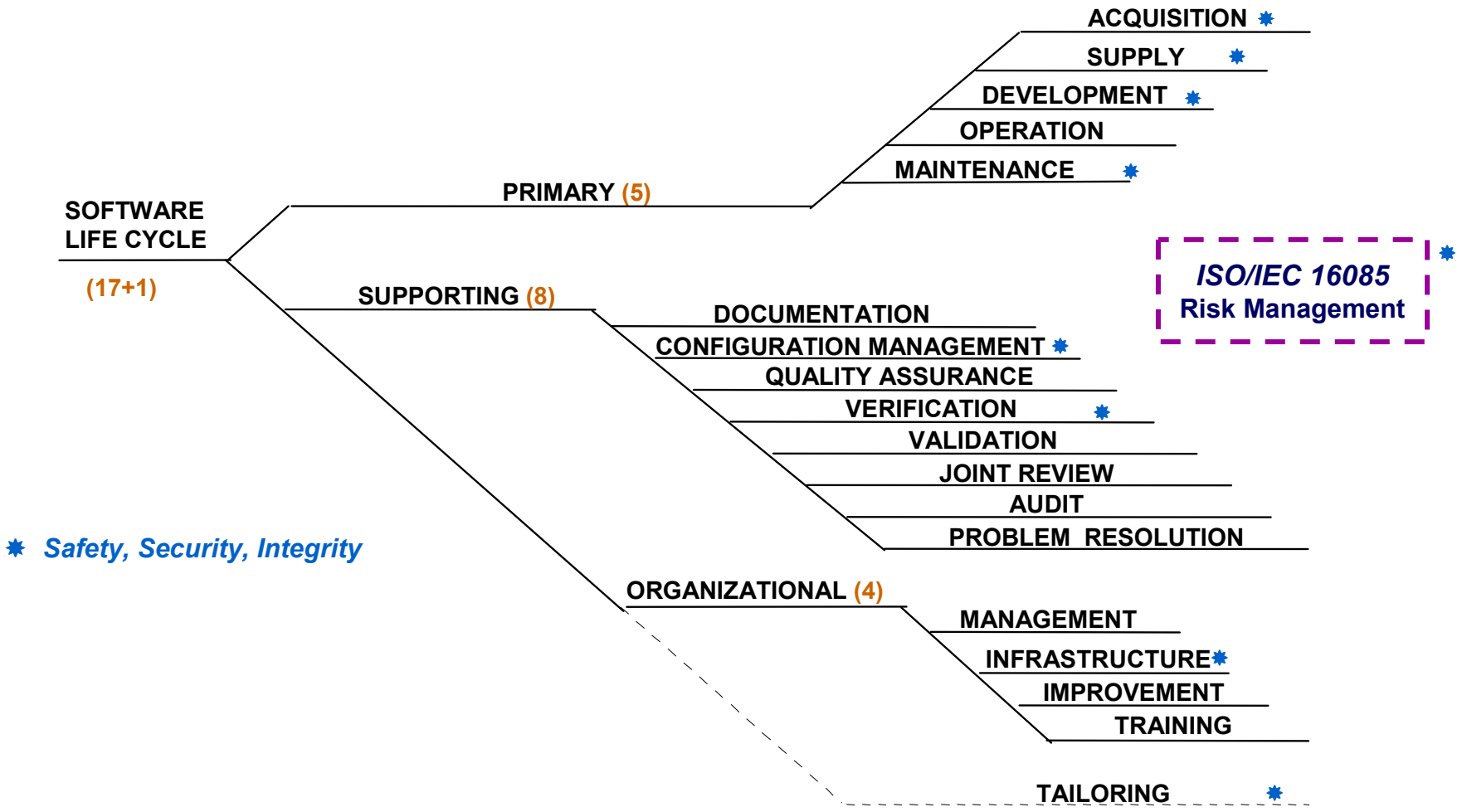
* Adopted from Paul Croll, Chairman of IEEE CS S2ESC and ISO SC7 WG9

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



Adapted from: Paul Croll, Chair, ISO/IEC JTC1/SC7 WG9, *ISO/IEC 15288, System Life Cycle Processes*, 2005.

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



Adapted from: Raghu Singh, *An Introduction to International Standards ISO/IEC 12207, Software Life Cycle Processes*, 1997.

Context for IT/Software Security

The environment consists of a changing set of conditions, Policies, and other factors often 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

Scope of ISO/IEC 15026 "System and Software Assurance"

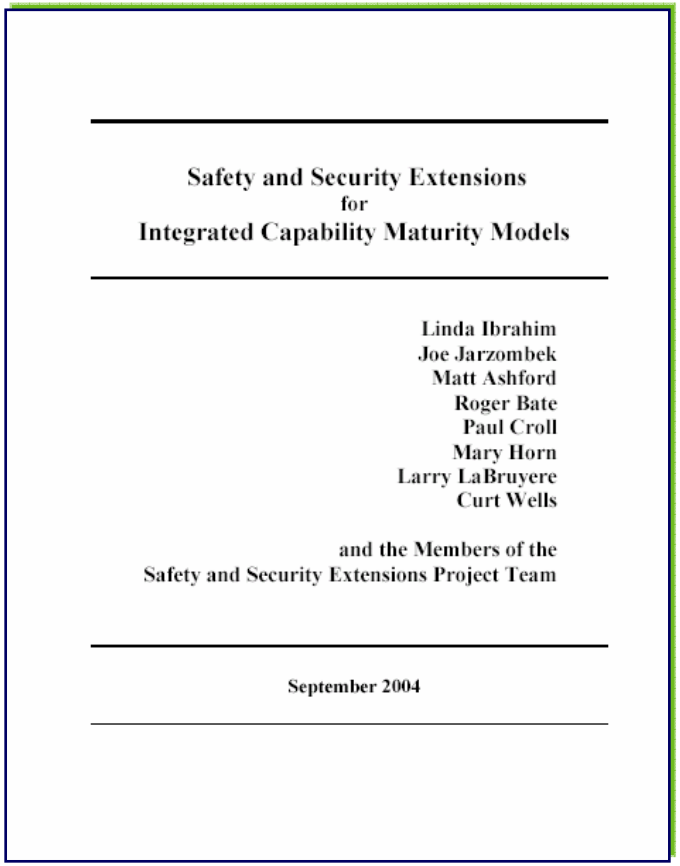
"System and software assurance focuses on the management of risk and assurance of safety, security, and dependability within the context of system and software life cycles."

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

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

"Safety & Security Extensions for Integrated Capability Maturity Models" – Input to 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



Safety and Security Extensions
for
Integrated Capability Maturity Models

Linda Ibrahim
Joe Jarzombek
Matt Ashford
Roger Bate
Paul Croll
Mary Horn
Larry LaBruyere
Curt Wells

and the Members of the
Safety and Security Extensions Project Team

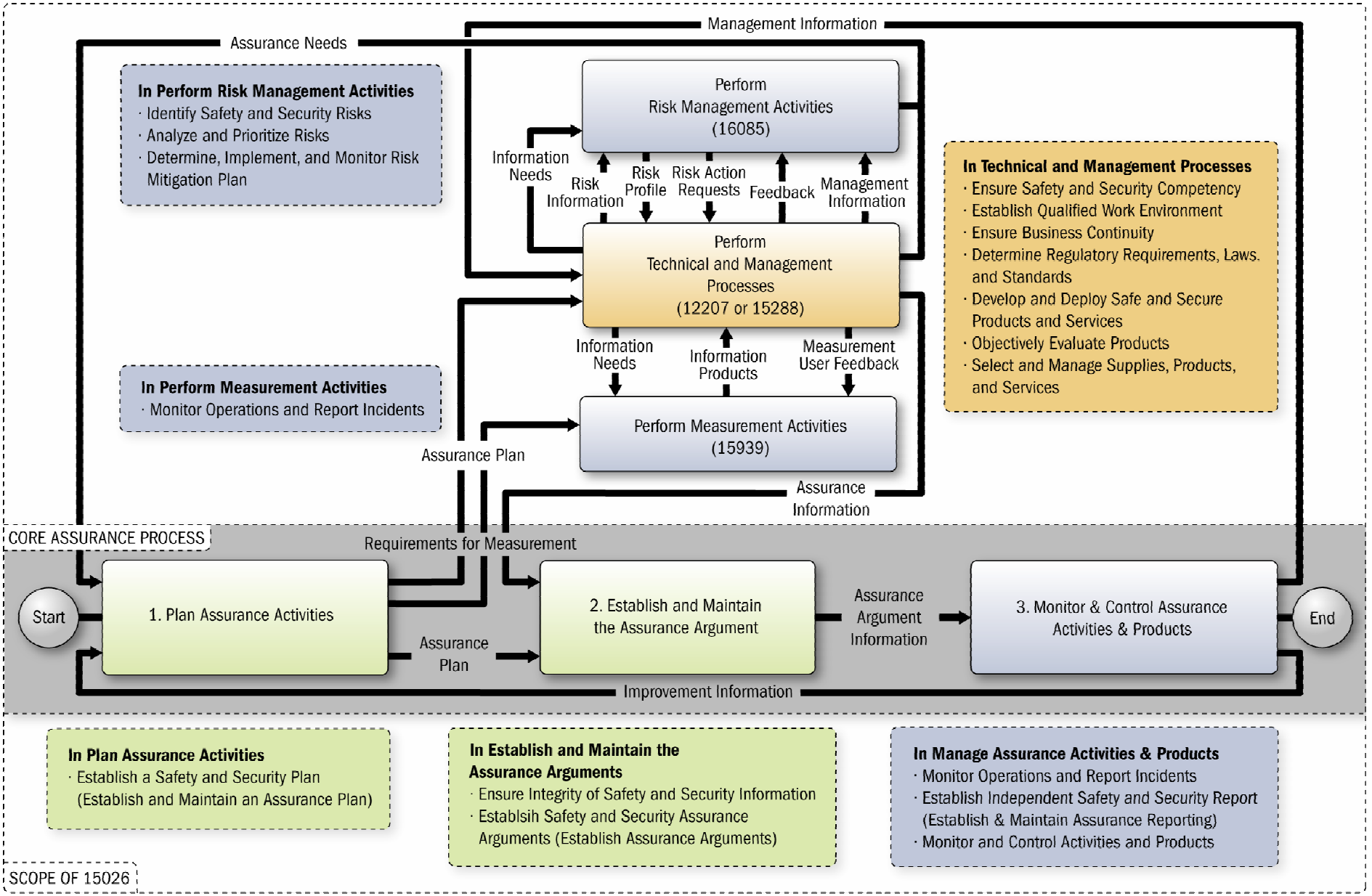
September 2004

www.faa.gov/ipg

Source: United States Department of Defense and Federal Aviation Administration joint project on, Safety and Security Extensions for Integrated Capability Maturity Models, September 2004

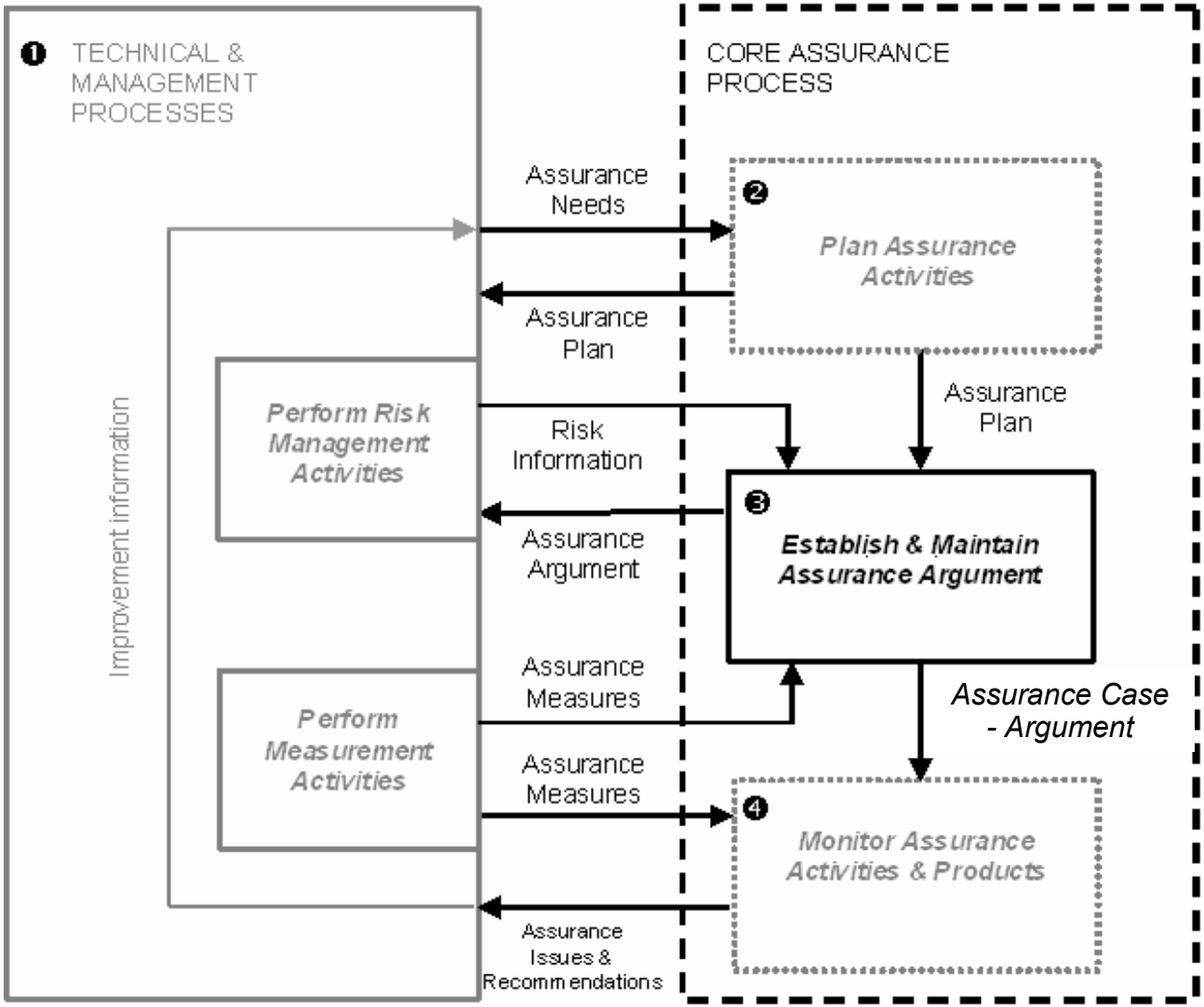
From synthesis and harmonization of practices from 8 standards (4 on security and 4 on safety)

ISO/IEC 15026 Framework for System & SW Assurance



ISO/IEC 15026 – System and Software Assurance
Interface with ISO/IEC Standards – Assurance Case/Argument

- Describes interfaces/ amplifications to the Technical & Management processes of ISO/IEC 15288 System Lifecycle & 12207 Software Lifecycle
- Describes interfaces/ amplifications to ISO/IEC 16085 Risk Management Process and 15939 Measurement Process and ISO/IEC 27004 Security Metrics
- Establishes centrality of the Assurance Argument
- Leverages IT security concepts and terminology in ISO/IEC15443
- Leverages OMG's ADM Task Force – Knowledge Discovery Meta-model



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

The Assurance Case/Argument – Requires Measurement

- Set of structured assurance claims, supported by evidence and reasoning, that demonstrates how assurance needs have been satisfied.
  - Shows compliance with assurance objectives
  - Provides an argument for the safety and security of the product or service.
  - Built, collected, and maintained throughout the life cycle
  - Derived from multiple sources
- Sub-parts
  - A high level summary
  - Justification that product or service is acceptably safe, secure, or dependable
  - Rationale for claiming a specified level of safety and security
  - Conformance with relevant standards and regulatory requirements
  - The configuration baseline
  - Identified hazards and threats and residual risk of each hazard and threat
  - Operational and support assumptions

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

The Assurance Case/Argument

Structure

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

Part 2: A set of supporting evidence
…
…

Attributes

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

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

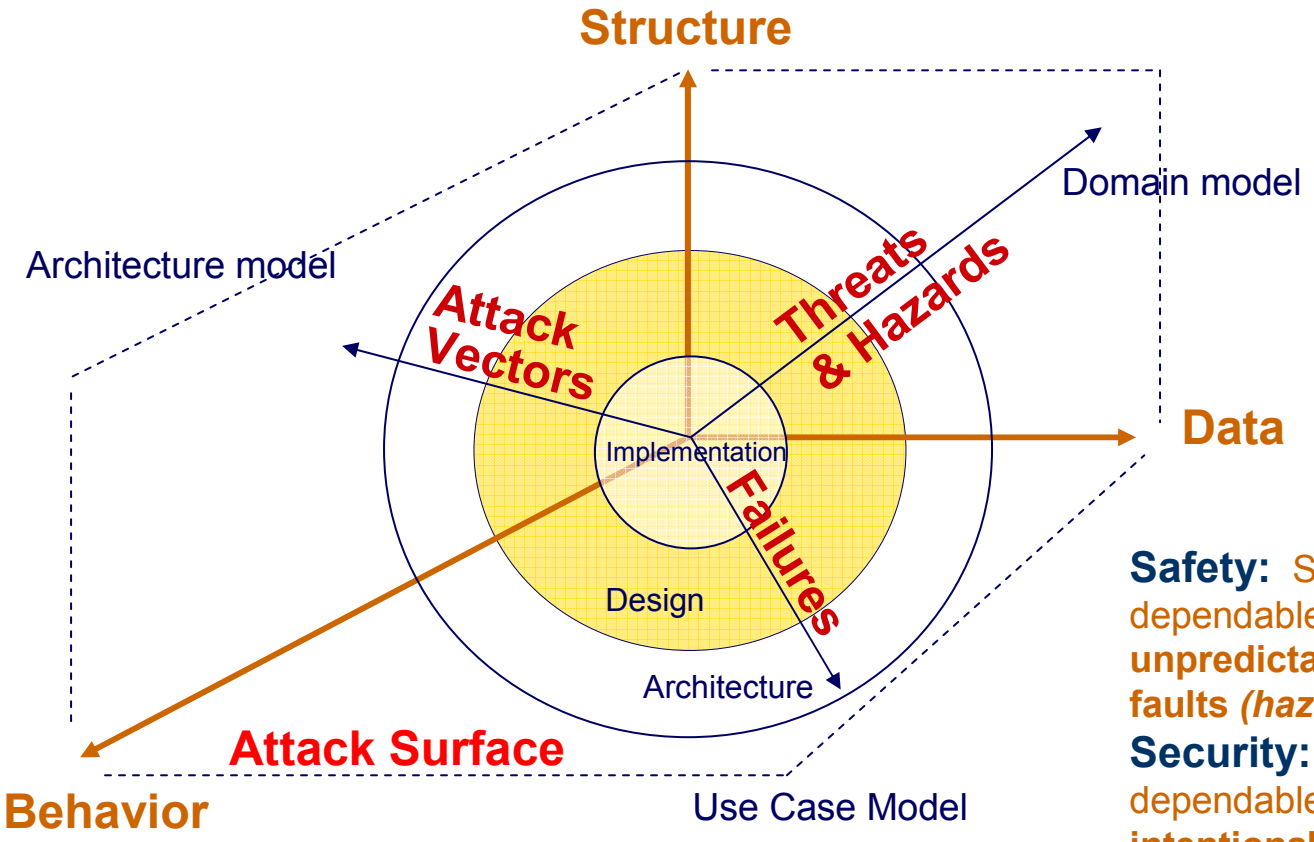
Key Standards for Software & System Processes

- 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

Partition of Concerns in Software-Intensive Systems



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

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

Considerations for Assurance Arguments:

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

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

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

Framework for IT Security Assurance

- **JTC1/SC 27 ISO/IEC TR 15443, Information technology -- Security techniques -- A framework for IT security assurance -- Part 1: Overview and framework**
  - Guides selection of an appropriate assurance method when specifying, selecting, or deploying a security service, product, or environmental factor such as an organization or personnel (known as a *deliverable*).
  - Facilitates the understanding of the assurance type and effort required to achieve confidence that the deliverable satisfies stated IT security assurance requirements and security policy.
  - Describes fundamentals of security assurance and relation to other security concepts.
    - Clarifies why security assurance is required and dispels misconceptions that increased assurance is gained by increasing the strength of security mechanisms.
    - Includes a categorization of assurance types and a generic lifecycle model to identify the appropriate assurance types required for the deliverable.
      - Demonstrates how security assurance must be managed throughout the deliverable's lifecycle requiring assurance decisions to be made by several assurance authorities for the lifecycle stage relevant to their organization (i.e. developer, standards, consumer).
      - Accommodates different assurance types and maps into any lifecycle approach so as not to dictate any particular design.
  - Includes advanced security assurance concepts, such as combining security assurance methods.

Framework for IT Security Assurance (cont.)

- ISO/IEC Technical Report 15443 addresses (within three parts):
  - ***Part 1, Overview and Framework*** provides fundamental concepts and general description of assurance methods:
    - Targets IT security in developing a security assurance program, determining the security assurance of deliverables, entering assurance assessment audits (e.g. ISO 9000, ISO/IEC 21827, ISO/IEC 15408-3), or other assurance activities.
  - ***Part 2, Assurance Methods*** describes a variety of assurance methods and approaches and relates them to Part 1 security assurance framework model:
    - Identifies qualitative properties of assurance methods.
    - Aids in understanding how to obtain assurance in a given life cycle stage of deliverable.
  - ***Part 3, Analysis of Assurance Methods*** analyzes the various methods with respect to their assurance properties and aids Assurance Authorities:
    - in deciding relative value of Assurance Approaches and determining that they will provide the assurance results most appropriate to their needs.
    - to use assurance results to achieve desired confidence of the deliverable.

ISO/IEC TR 15446 – Additional guidance with applicable concepts specifying security claims

- ISO/IEC TR 15446:2004, Information technology -- Security techniques -- Guide for the production of Protection Profiles and Security Targets
  - Provides guidance relating to the construction of Protection Profiles (PPs) and Security Targets (STs) that are intended to be compliant with ISO/IEC 15408 (the "Common Criteria").
    - Gives suggestions on how to develop each section of a PP or ST.
    - Supported by an annex that contains generic examples of each type of PP and ST component, and by other annexes that contain detailed worked examples.
  - Is primarily aimed at the development of PPs and STs.
    - Is likely to be useful to evaluators of PPs and STs and to those who are responsible for monitoring PP and ST evaluation.
    - May also be of interest to consumers and users of PPs and STs who wish to understand what guidance the PP/ST author used, and which parts of the PP or ST are of principal interest.

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

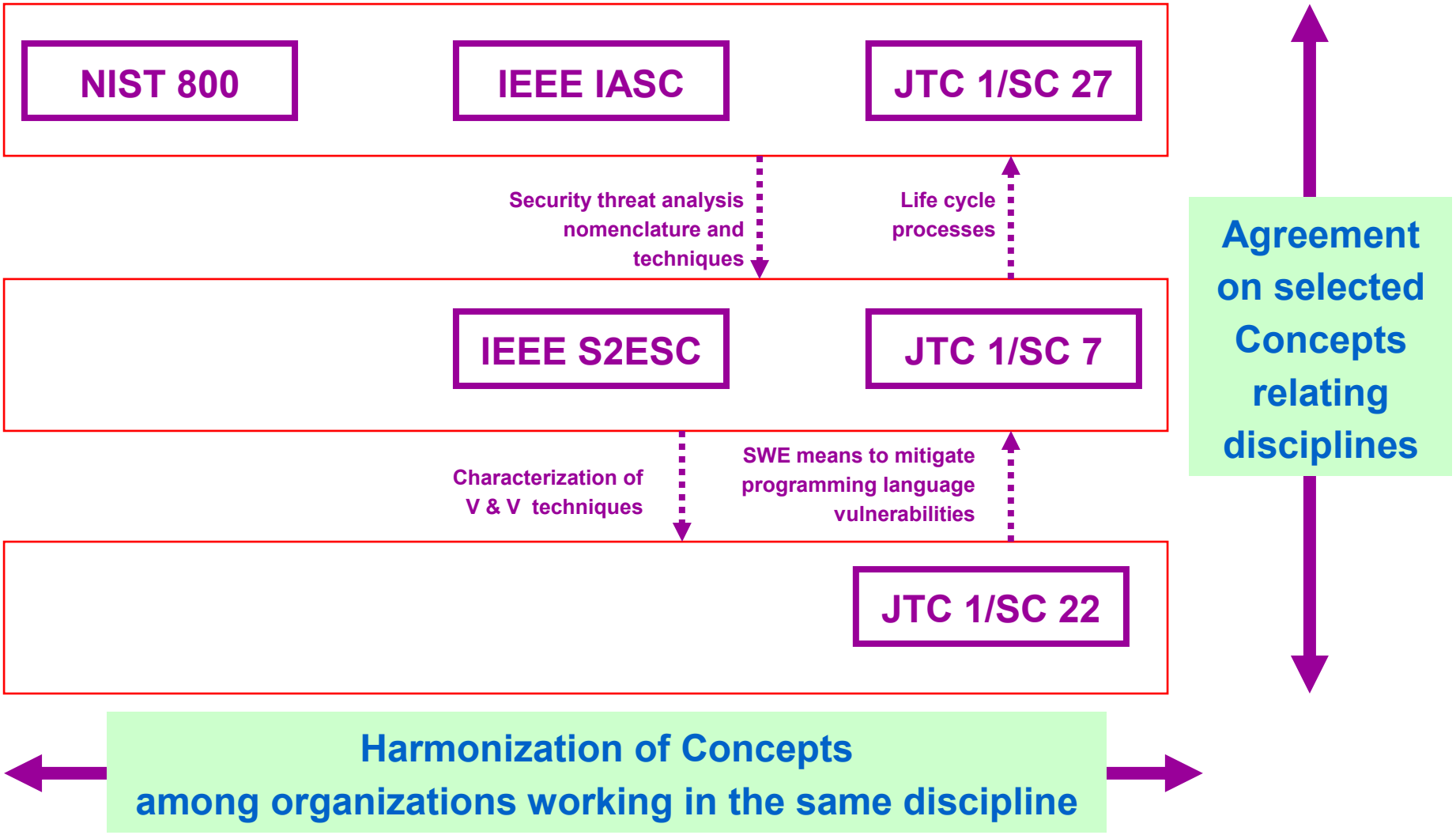
- Process of building *trust* … embodied in software asset evaluation
- *Claims* about software systems…
  - Involve certain *Target Requirement* (intentions)
    - Related to *risks*
    - How vendor-specified risk is mitigated
    - Security requirements
    - Process requirements (cleanroom, ISO, 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

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.)
  - Agreed-upon ways to interpret such claims, properties, etc. (common meaning, as opposed to simply common format).
  - Archives of such claims (libraries, repositories) that allow search, comparison, etc. (which again needs shared taxonomy, etc.)
  - Automated methods (supported by tools)

Homeland Security

Examples of Desired Relationships



* Adopted from Jim Moore, IEEE CS S2ESC Liaison to ISO SC 7

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.

Homeland Security

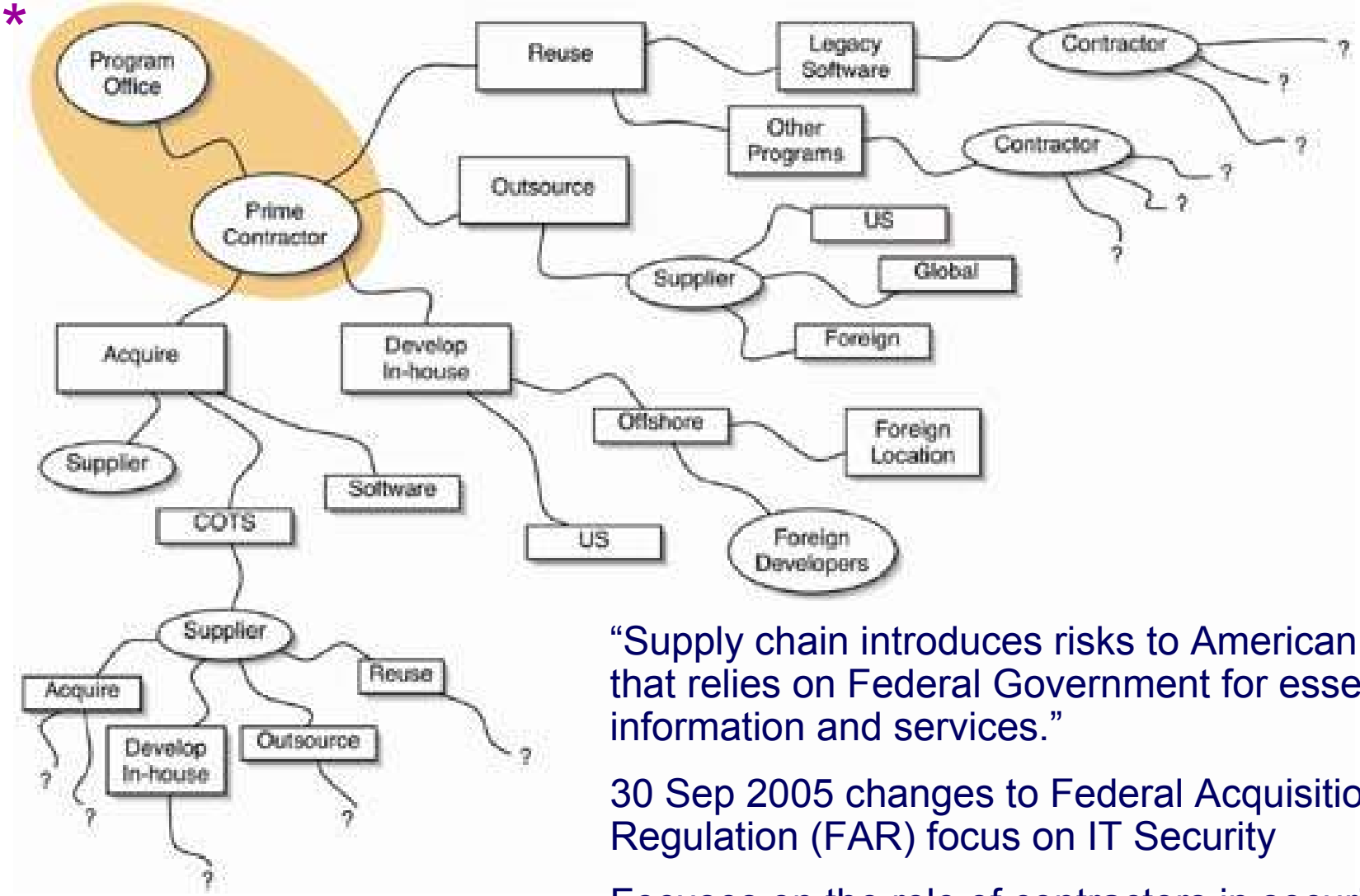
DHS Software Assurance: Acquisition

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

Homeland Security

**NCSD Objective/Action 1.4.4

*



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

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

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

Homeland Security

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

FISMA IT security provisions now in FAR

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

Homeland Security

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

NIST Enterprise Risk Management Framework

FIPS 199 / SP 800-60

Starting Point

Security Categorization

Defines category of information system according to potential impact of loss

SP 800-53 / FIPS 200

Security Control Selection

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

SP 800-37

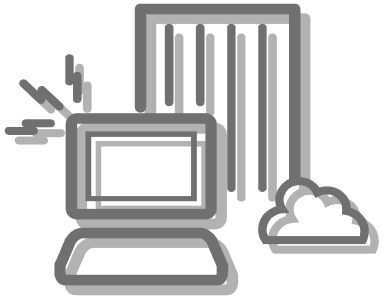
Security Control Monitoring

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

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

Security Control Refinement

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



SP 800-37

System Authorization

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

SP 800-18

Security Control Documentation

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

SP 800-70

Security Control Implementation

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

SP 800-53A / SP 800-37

Security Control Assessment

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

Homeland Security

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

DHS Software Assurance: Technology

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

Homeland Security

**NCSD Objective/Action 1.4.3

SwA Metrics & Tool Evaluation (SAMATE)

* SAMATE Reference Dataset (SRD), version 2, on-line

  This dataset will have 1000s of test cases for evaluation and development of SwA tools. Cases will have breadth of

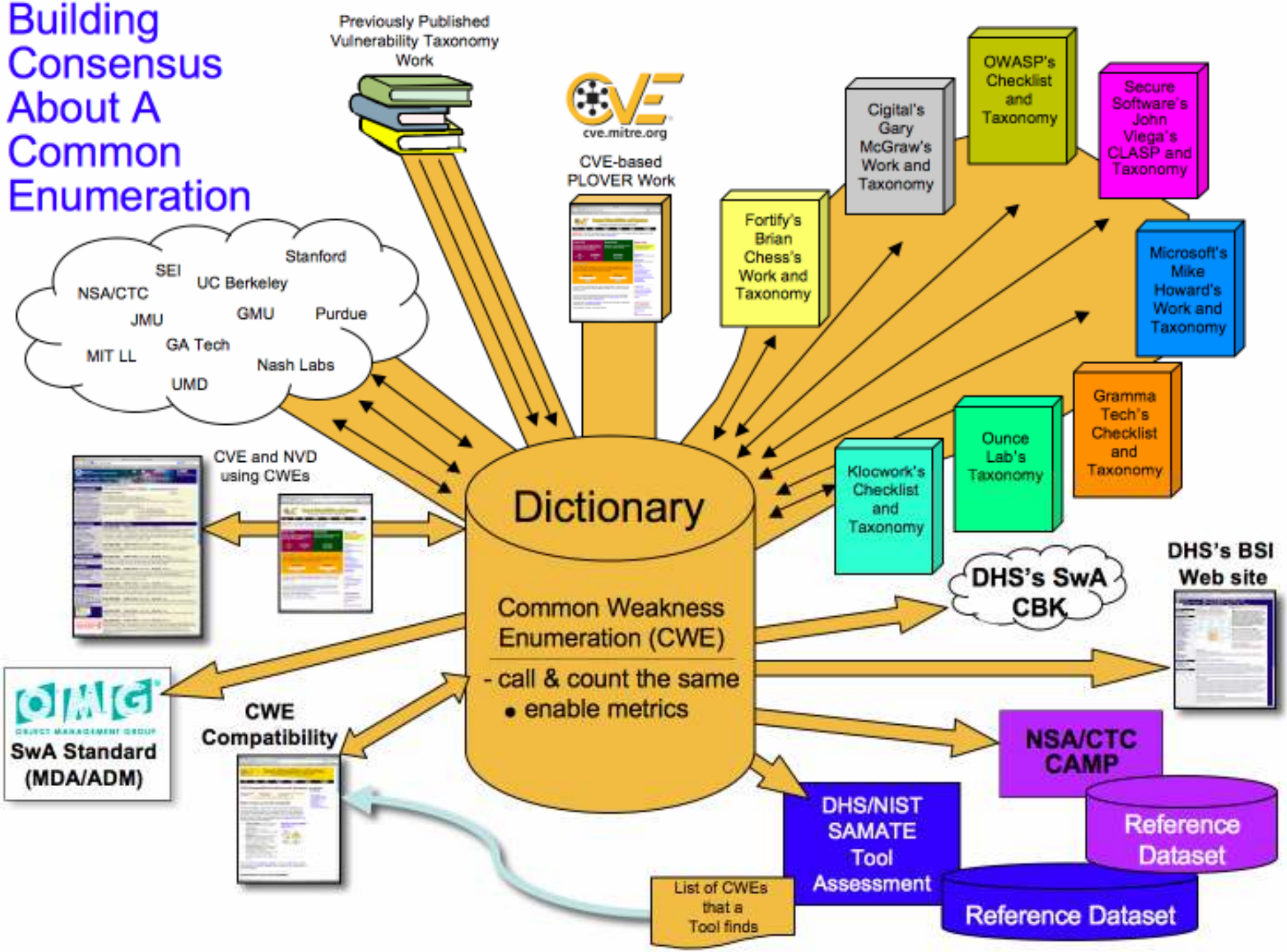
  - language (C, Java, UML, etc.)
  - life cycle (design model, source code, application, ...)
  - size and type (small and huge, production and artificial, ...)

* Specifications and a reviewed test, including a suite of test cases (from the SRD above) for one class of SwA tool, probably source code scanners.
* Specifications & test for another class of SwA tool, probably web applications.
* Establish an advisory committee and create a road map to creating tests for all SwA tools (which tool classes should be done first?).
* List SwA areas with underdeveloped tools; sketch R&D that could fill each area.
* Requires Common Enumeration of Weaknesses to provide a dictionary of software flaws

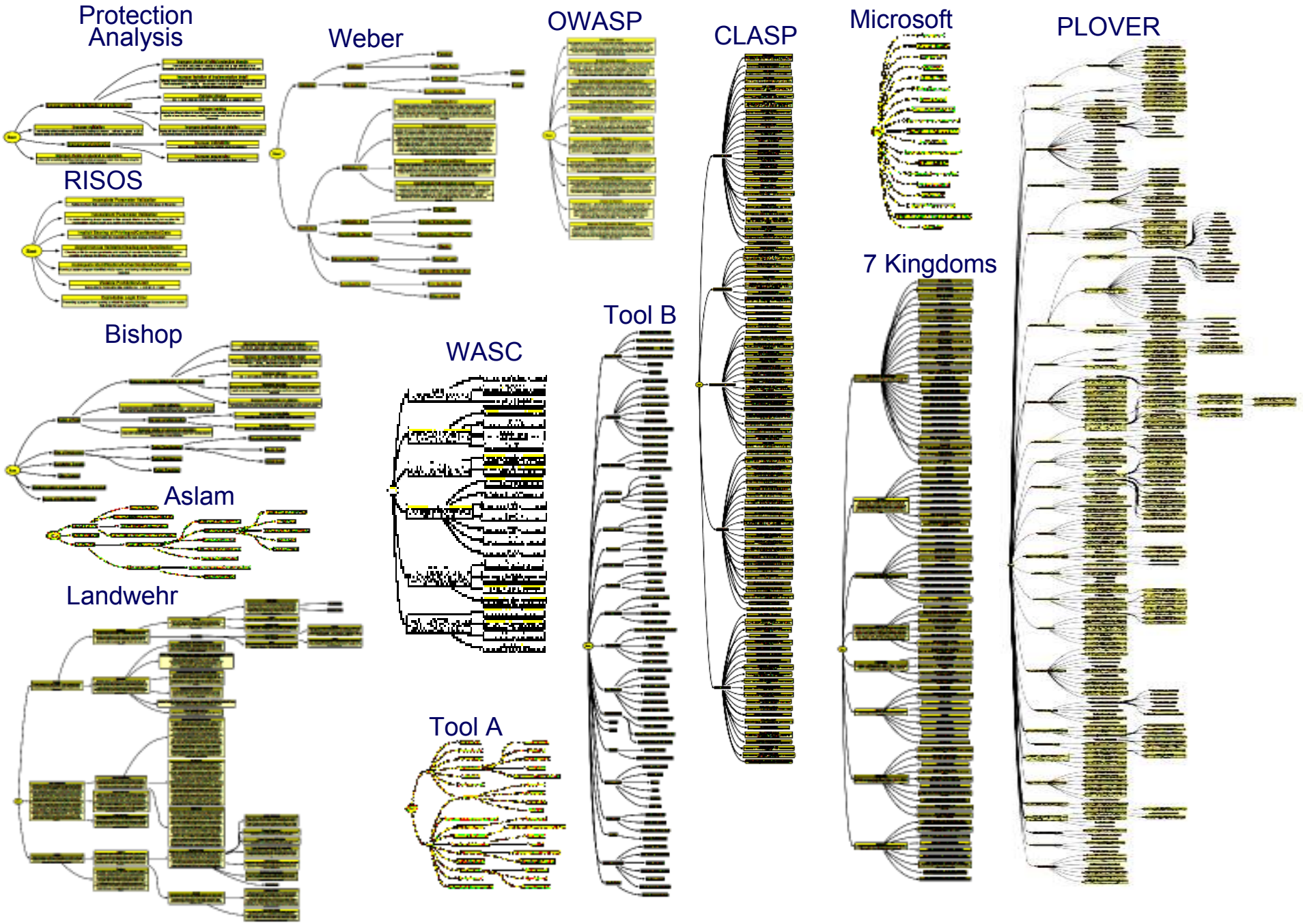
Homeland Security

SAMATE project leader, Paul E. Black, paul.black@nist.gov (p.black@acm.org),
100 Bureau Drive, Stop 8970, Gaithersburg, Maryland 20899-8970
voice: +1 301 975-4794, fax: +1 301 926-3696, http://hissa.nist.gov/~black/

Building Consensus About A Common Enumeration



Taxonomies Contributing to Common Flaw Enumeration

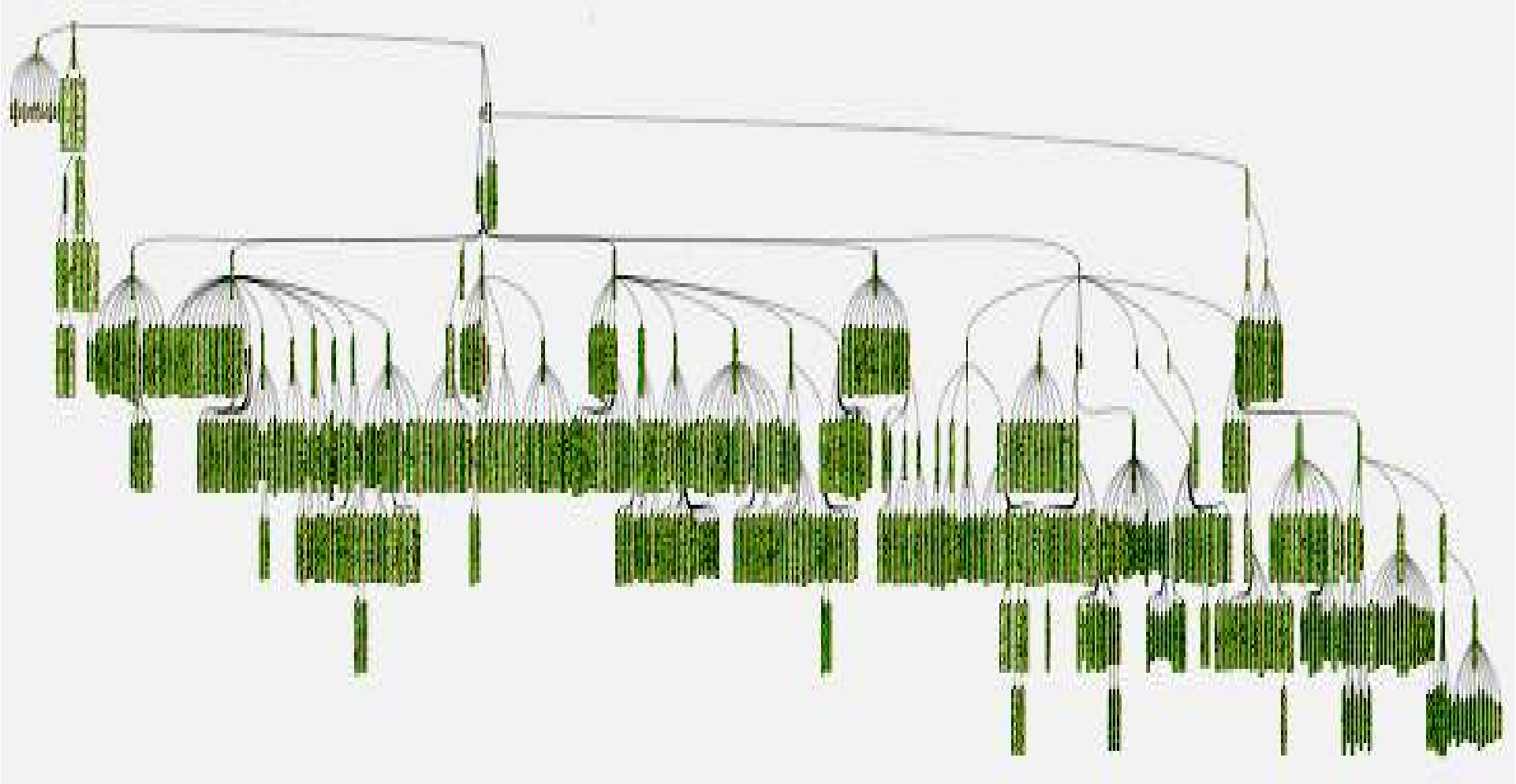


Current Community Contributing to the Common Flaw Enumeration

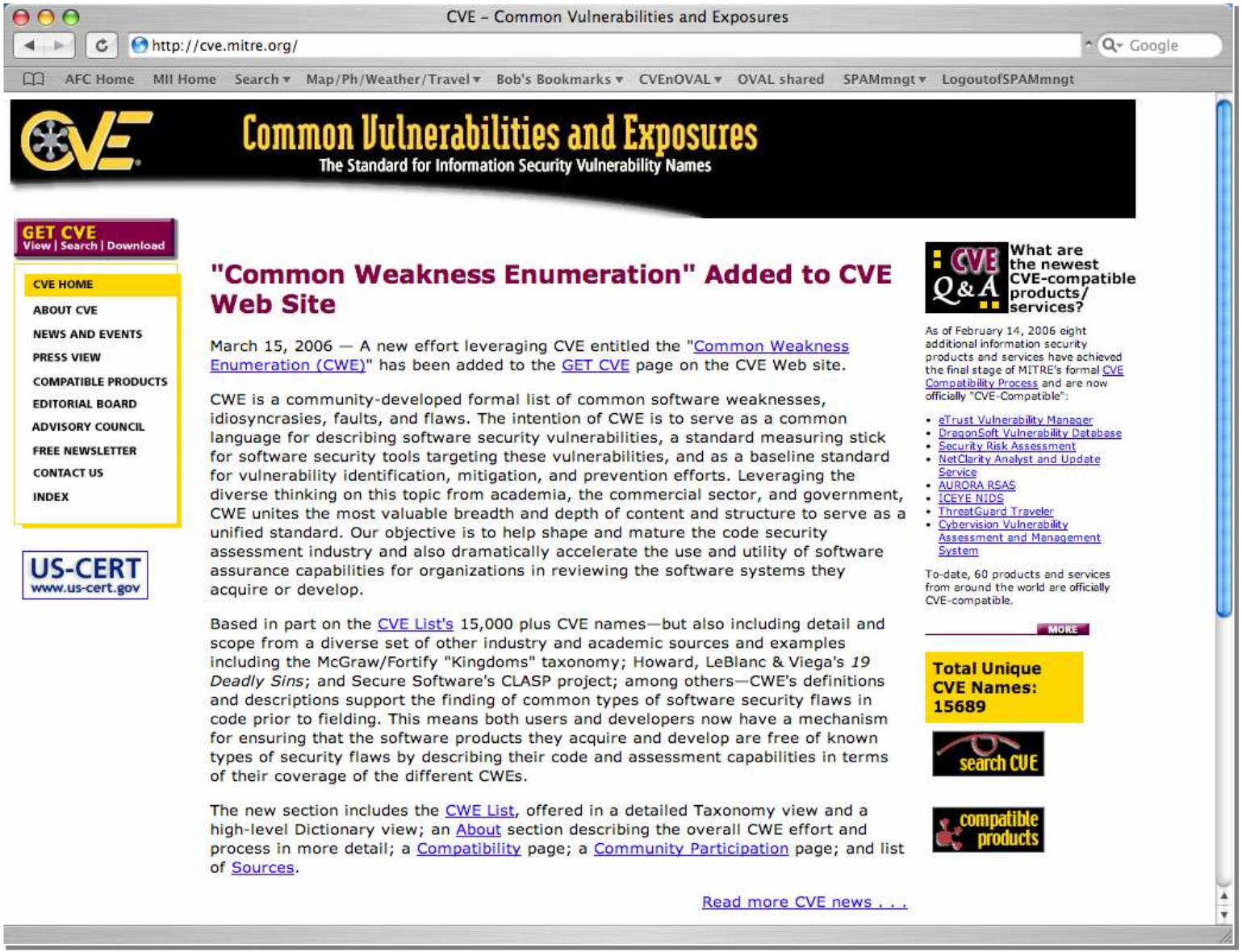
- Cenzic
- CERT/CC
- Cigital
- CodescanLabs
- Coverity
- DHS
- Fortify
- IBM
- Interoperability Clearing House
- JHU/APL
- Kestrel Technology
- Klocwork
- Microsoft
- MIT Lincoln Labs
- MITRE
- North Carolina State University
- NIST
- NSA
- Oracle
- Ounce Labs
- OWASP
- PARASOFT
- Secure Software
- Security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

- Tim Newsham

Approximately 500 Dictionary Elements



CWE Initial Draft is available



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

Common Attack Patterns Enumeration and Classification (CAPEC)

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

Homeland Security

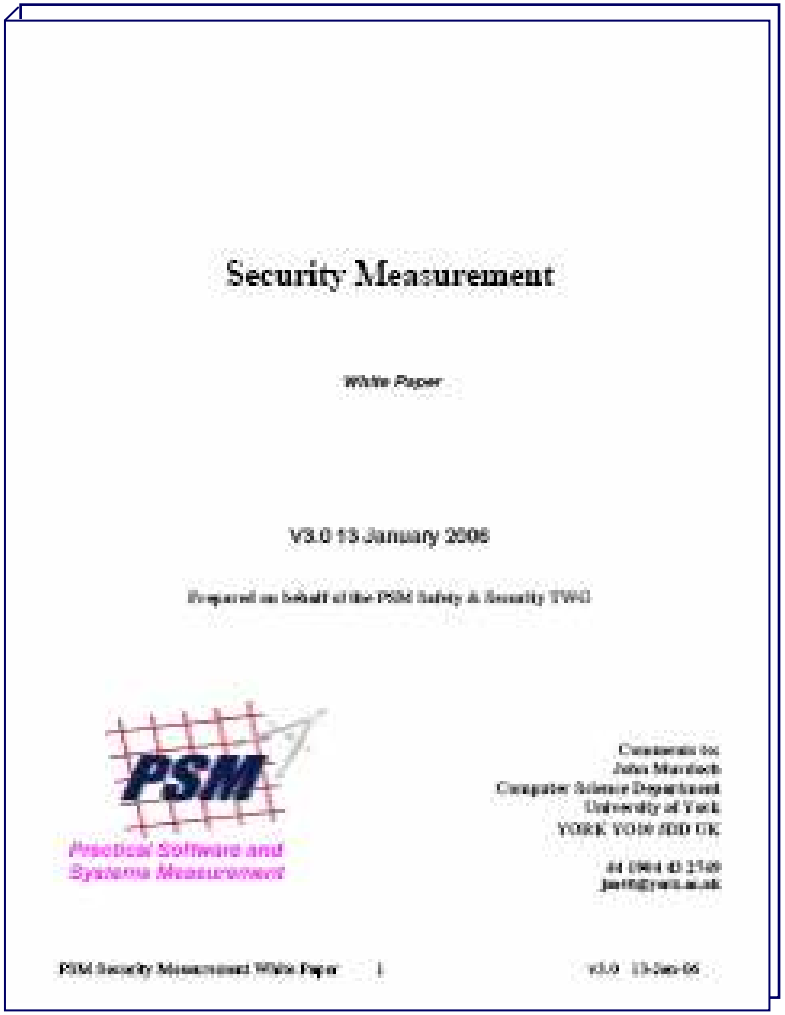
Common Attack Patterns Enumeration and Classification (CAPEC)

- **CAPEC Service Deliverables**
  - Primary catalog deliverable
  - Common Attack Pattern Enumeration and Classification XML document
  - Attack Pattern schema description document
  - Attack Pattern XML schema document
  - Attack Pattern Classification Taxonomy XML document
  - References list document
  - Interim work product deliverables
  - Operational Support element deliverables
  - Conference/workshop presentations on CAPEC
  - CAPEC extension and sustainment process document

Homeland Security

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

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



Homeland Security

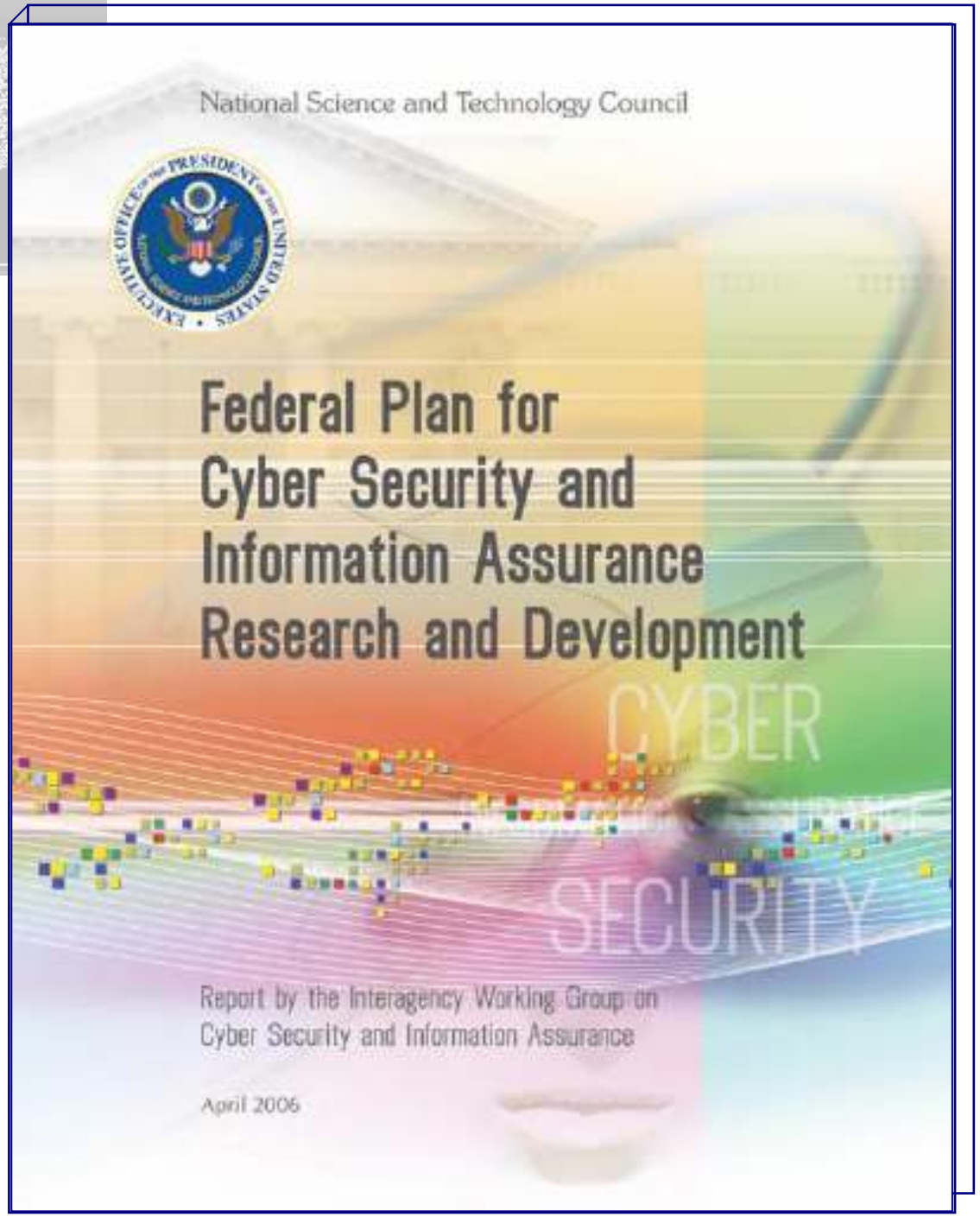
www.psmsc.com

Software Assurance R&D

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

Homeland Security

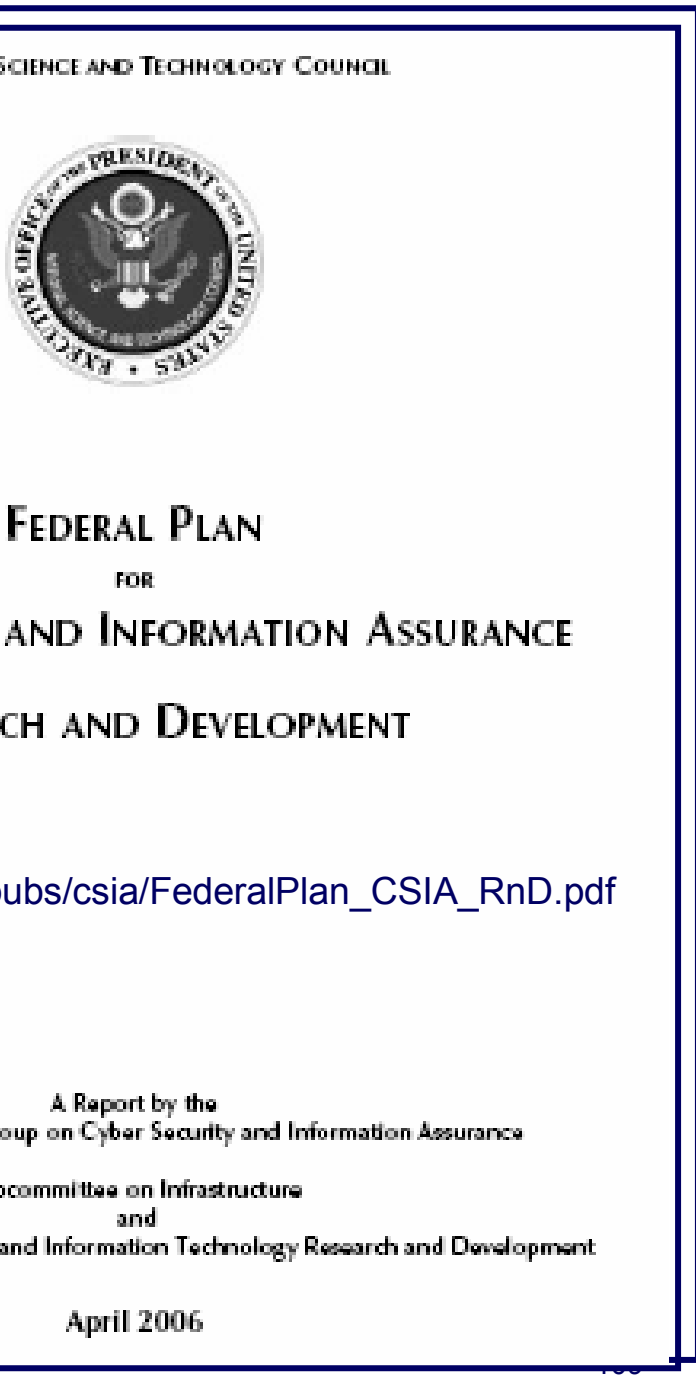
http://www.nitrd.gov



Homeland Security

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

Homeland Security



NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

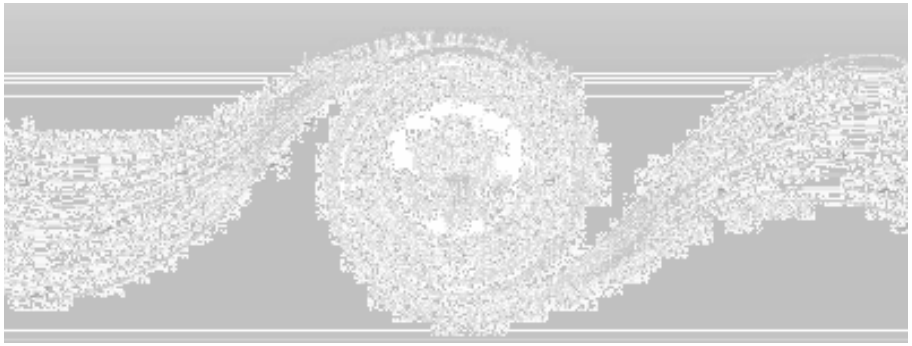
FEDERAL PLAN
FOR
CYBER SECURITY AND INFORMATION ASSURANCE
RESEARCH AND DEVELOPMENT

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

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

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

April 2006



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

Homeland Security

Top Priorities Technical / Funding

Attack protection, prevention, & preemption

Automated attack detection, warning & response

Secure process control systems

Wireless security

Software quality assessment & fault characterization

Software testing & assessment tools

Secure software engineering

Analytical techniques for security across the IT systems engineering life cycle

Cyber Security & IA R&D testbeds

Trusted computing base architectures

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

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

Examining IT/Software Security Requirements

- How are common weaknesses/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?
- How can measurement be enhanced to better support decision-making associated with IT/software security?

Homeland Security

Bi-Monthly Software Assurance (SwA) Working Groups:

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

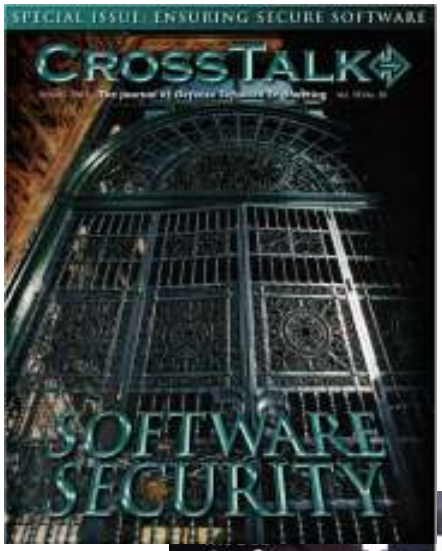
	Tuesday, July 18th	**Wednesday, July 19th**	**Thursday, July 20th**
Morning 9:00am - 11:30am	Session 1: Business Case WG	Plenary Session	Session 5: Acquisition WG
	Session 2: Processes/Practices (standards) WG		Session 6: Measurement WG
Afternoon 1pm - 5pm	Session 1: Business Case WG	Session 3: Technology,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

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

Homeland Security

DHS Software Assurance Outreach Services

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



INPUT TargetVIEW

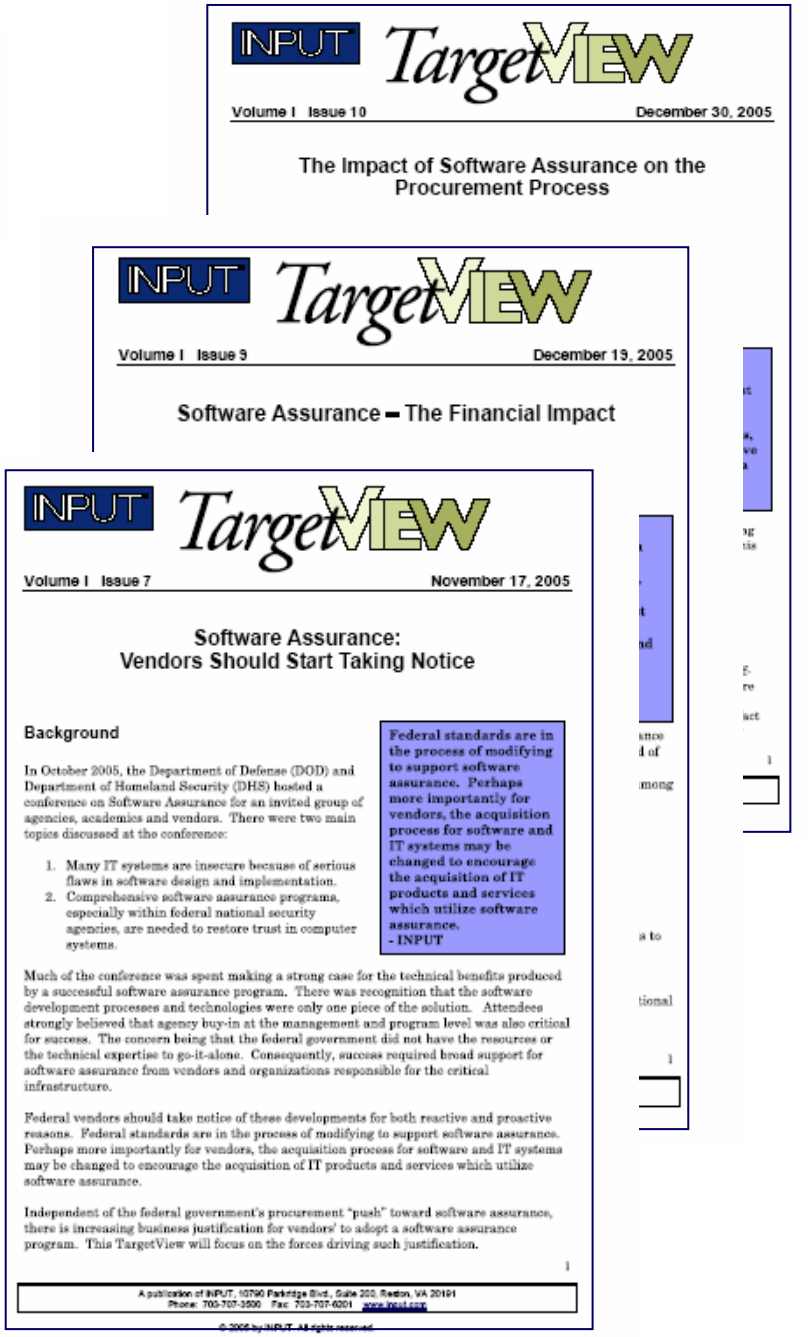
Homeland Security

INPUT TargetVIEW

The Impact of Software Assurance on the Procurement Process

Software Assurance – The Financial Impact

Software Assurance – Vendors Should Start Taking Notice



Homeland Security

Software Assurance Observations

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

Homeland Security

DHS Software Assurance Program

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

Homeland Security

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

Achieving Software Assurance – in the future

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

Semi-Annual Software Assurance Forum -- Next in 3 Oct 2006

www.us-cert.gov →

http://buildsecurityin.us-cert.gov

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

Homeland Security

Homeland Security

Questions?

- - - - - - - -

Back-up Slides

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.

Homeland Security

www.us-cert.gov

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.

Homeland Security

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

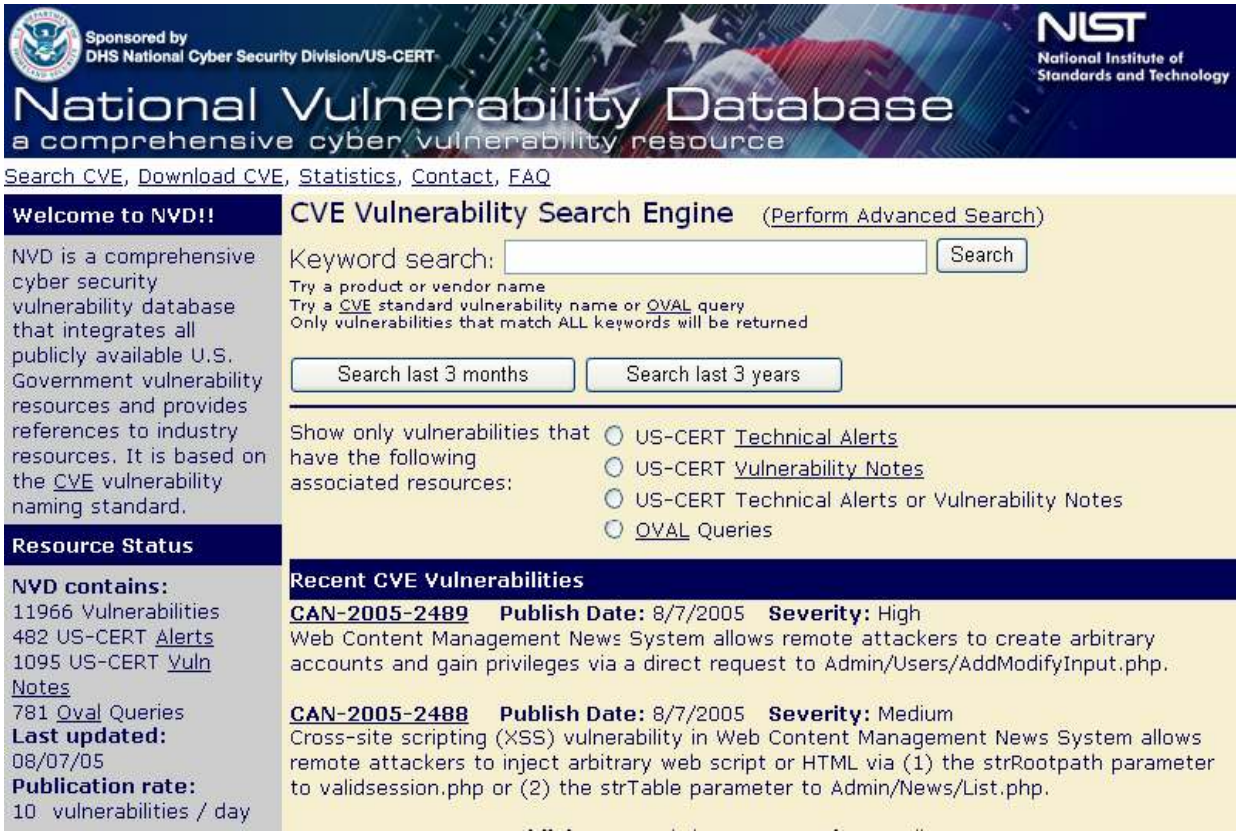
NVD Search Capability

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
- software name and version number
- vendor name
- 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



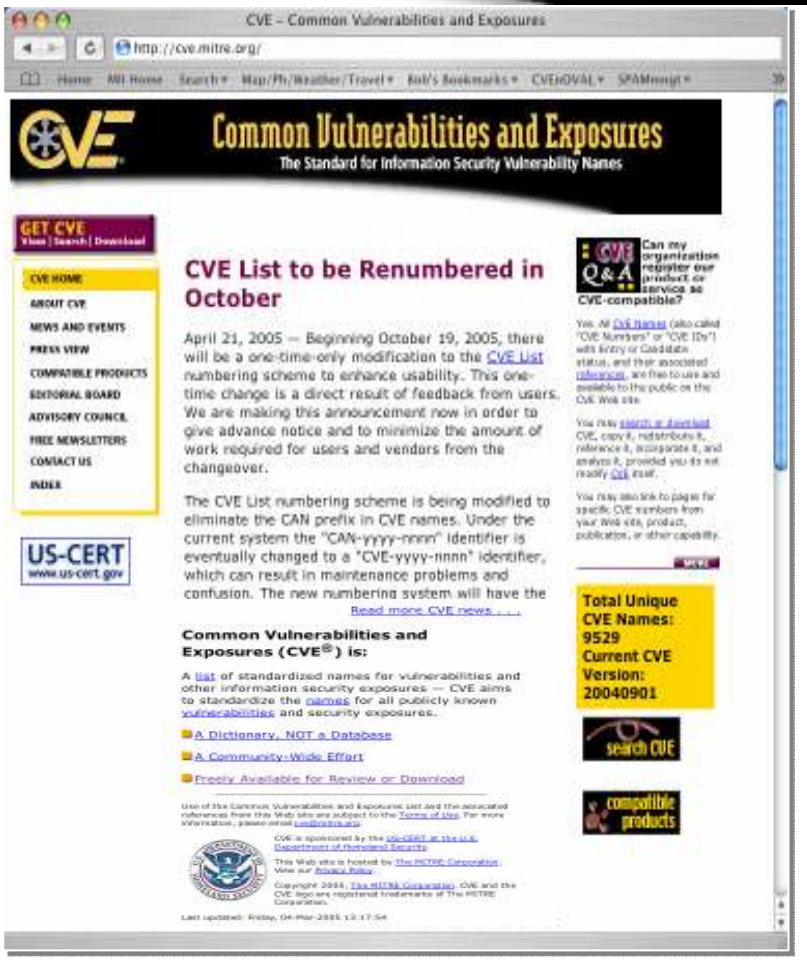
Homeland Security

http://nvd.nist.gov

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

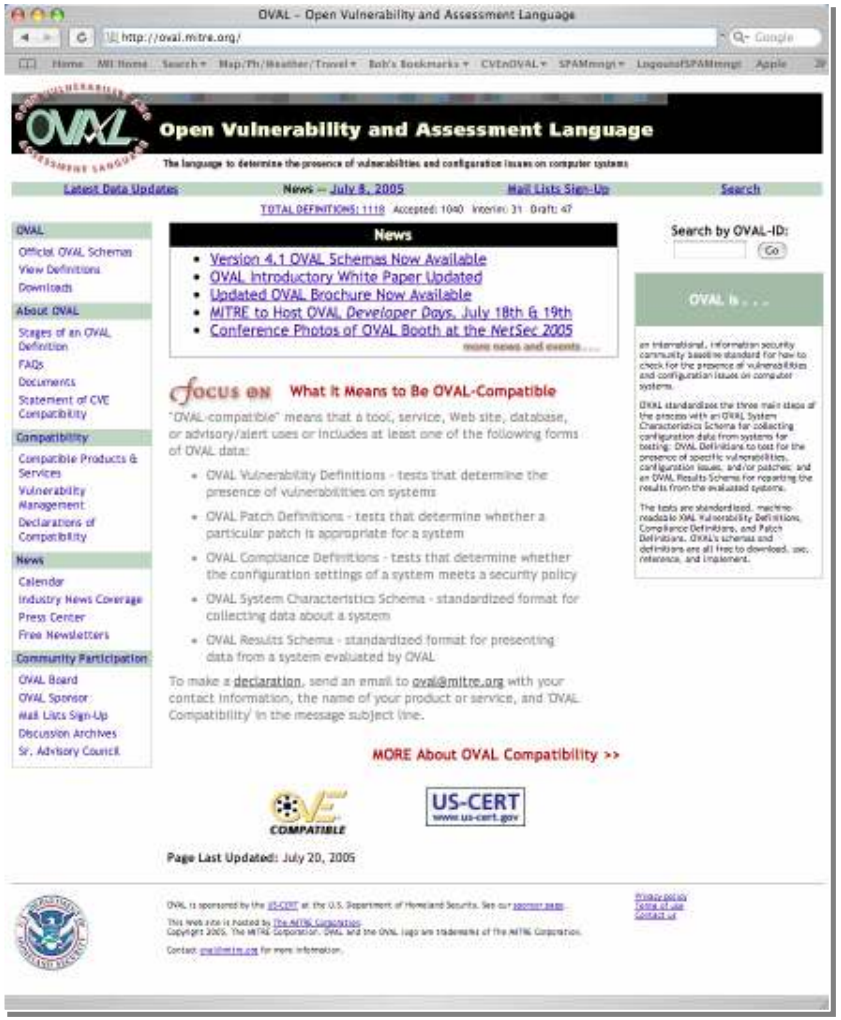
- An international security community activity
  - to provide common names for publicly known security vulnerabilities and exposures
- Key tenets
  - One name for one vulnerability or exposure
  - One standardized description for each
  - Existence as a dictionary
  - Publicly accessible on the Internet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



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



1,141 OVAL Definitions

http://oval.mitre.org
Public unveiling - December 2002

CME Common™ Malware Enumeration
Reducing Public Confusion During Malware Outbreaks

For CME Process (scope, identifiers & guidelines for deconfliction), see 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.

Homeland Security

Building on CVE and OVAL efforts