SOFTWARE ASSURANCE FORUM

Homeland Security

Commerce

National Defense

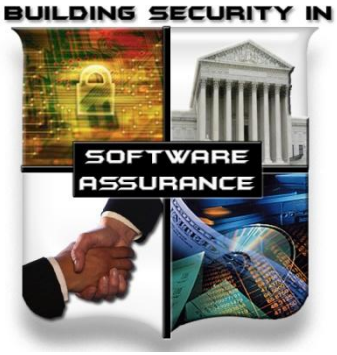
BUILDING SECURITY IN

Public/Private Collaboration Efforts for Software Supply Chain Risk Management

Next SwA Working Group Sessions 14-17 Dec 2010 at MITRE, McLean, VA

National CyberSecurity Awareness

STOP | THINK | CONNECT™



Cyber Assurance Ecosystem: Automation and Processes for Securing the Enterprises

Nov 10, 2010

Joe Jarzombek, PMP, CSSLP
Director for Software Assurance
National Cyber Security Division
Office of the Assistant Secretary for
Cybersecurity and Communications

Homeland Security

Understanding the Threat and Controlling the Attack

One who knows the enemy and knows himself will not be endangered in a hundred engagements.

One who does not know the enemy but knows himself will sometimes be victorious; sometimes meet with defeat.

One who knows neither the enemy nor himself will invariably be defeated in every engagement.

- **The Art of War, Sun Tzu**

An appropriate defense can only be established if one knows its weaknesses and how it will be attacked; thus controlling attack surface/vectors

- **Software Assurance Forum, Joe Jarzombek**

Homeland Security

OSWASP AppSecDC Software Assurance Track

10:45 -- Cyber Assurance Ecosystem: Automation and Processes for Securing the Enterprise

– Joe Jarzombek and Tom Millar (DHS NCSD)

11:35 -- Security Risk and the Software Supply Chain

– Karen Goertzel (BAH)

1:20 -- Understanding How They Attack Your Weaknesses

– CWE & CAPEC – Sean Barnum (MITRE)

3:10 -- Ensuring Software Assurance Process Maturity

– Ed Wotring (SRA)

4:00 -- People, Process, and Technology: OWASP impact on the SwA Processes and Practices WG

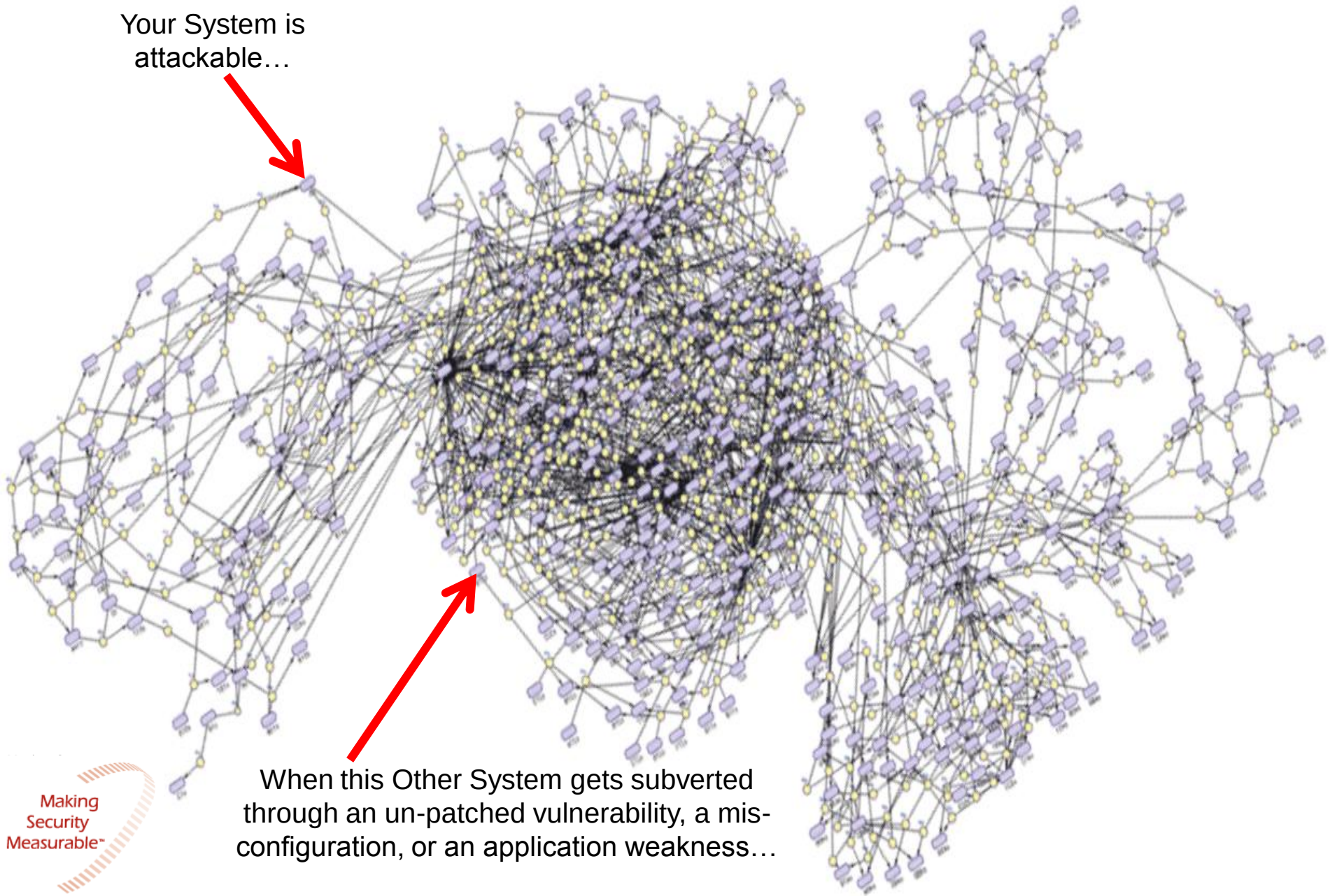
– Michele Moss (BAH)

4:50 -- Federal Perspective on Application Security -- Panel

Aligned with OWASP initiatives

- Secure Coding guideline, code review, testing guidance
- Security considerations for acquisition and procurement
- Open source modules that have been vetted relative to mitigation of common weaknesses
  - OWASP Infrastructure for Open Source Labs

Today Everything's Connected



Making Security Measurable™

Cyber Incidents are Increasing in Frequency, Scale, and Sophistication

From Times Online

August 11, 2008

Georgia accuses Russia of waging 'cyber-war'

Several
the exte

Jonathan

Georgia to
using hack
websites

Hackers Update Conficker Worm, Evade Countermeasures

Gregg Keizer, Computerworld

Tuesday, March 10, 2009 7:17 AM PDT

TJX theft tops 45.6 million card numbers

Robert Lemos, SecurityFocus 2007-03-30

each of its systems, retail
best guess at the number
and other data were stolen

ards had been stolen by
ompany's computer
y 2005 and mid-January

Government computers under attack

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

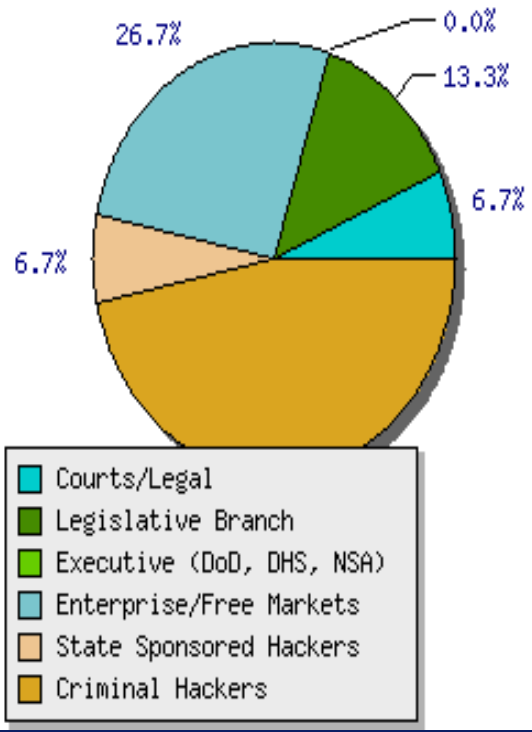
Greg Masters February 17, 2009

Records show that cyberattacks on federal computer networks increased 40 percent last year, and that figure is likely low as it reflects on the reported attacks.

Based on data provided to *USA Today* by US-CERT, unauthorized access to government computers and installations of hostile programs rose from a combined 3,928 incidents in 2007 to 5,444 in 2008.

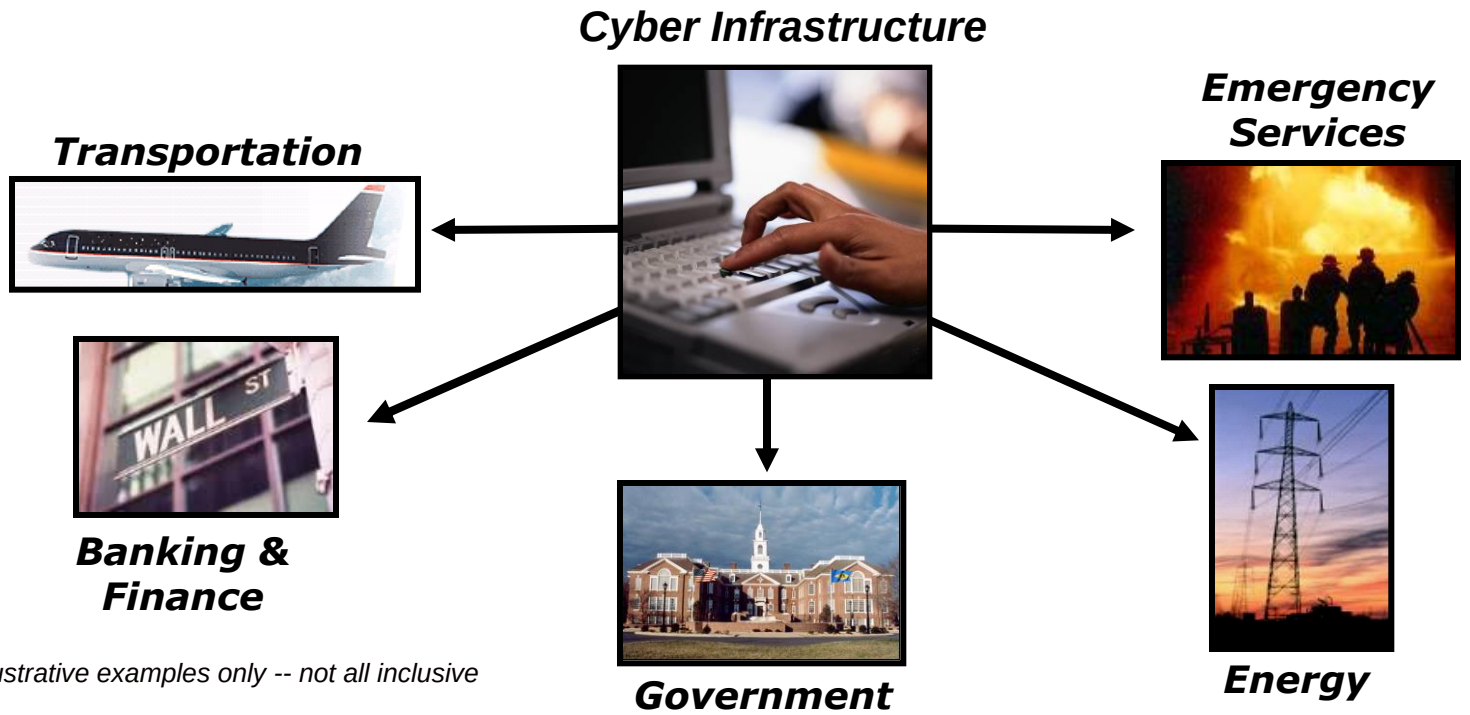
Latest Survey Results:

Hackers will have the most impact on shaping information security over the next decade



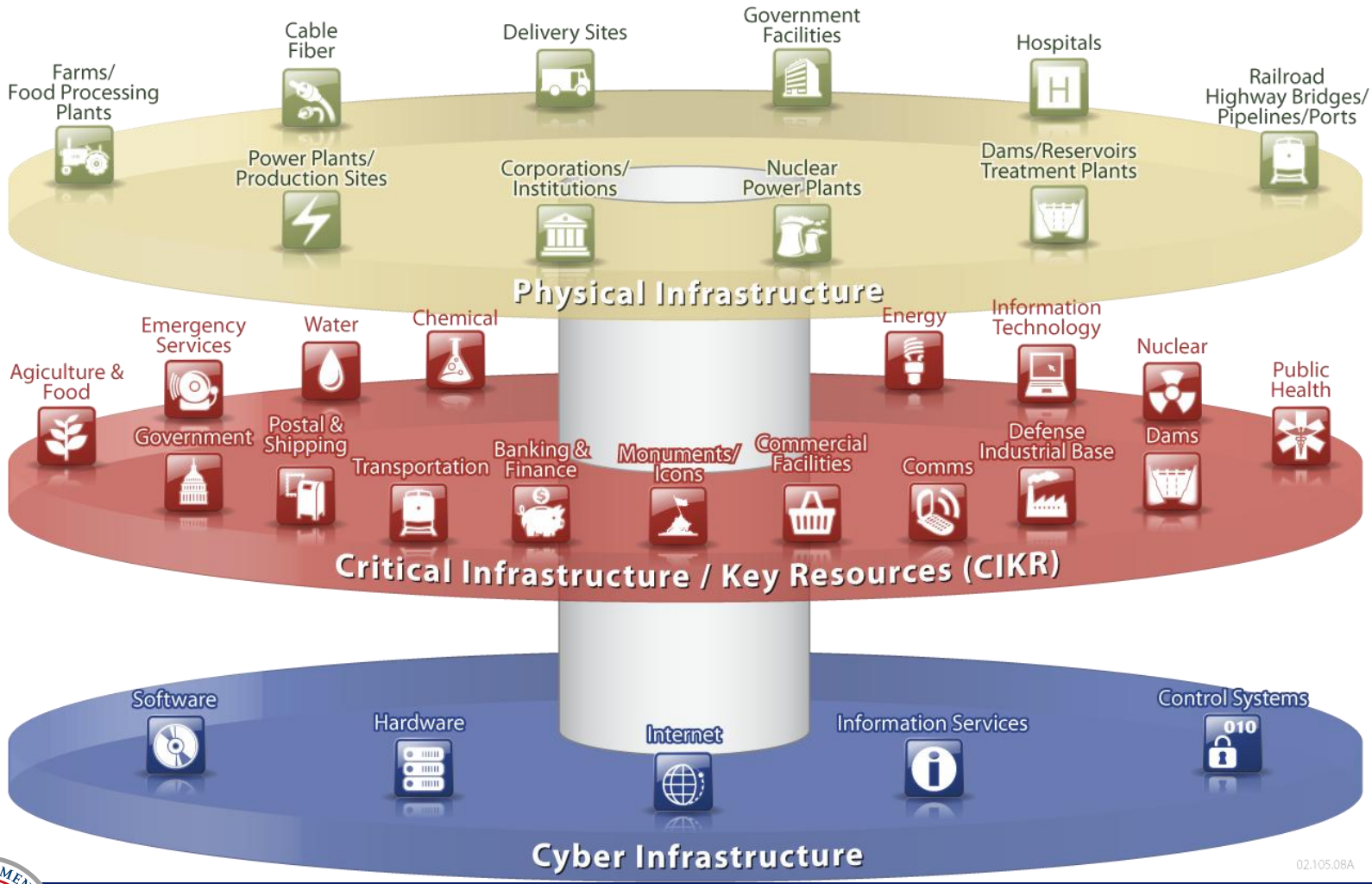
Cyber Infrastructure: Critical to National and Economic Security

Cyber Infrastructure represents the convergence of information technology and communications systems, is inherent to nearly every aspect of modern life

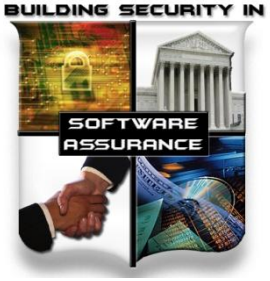


Illustrative examples only -- not all inclusive

Interdependencies Between Physical and Cyber Infrastructures -- Need for secure software applications



Critical Considerations



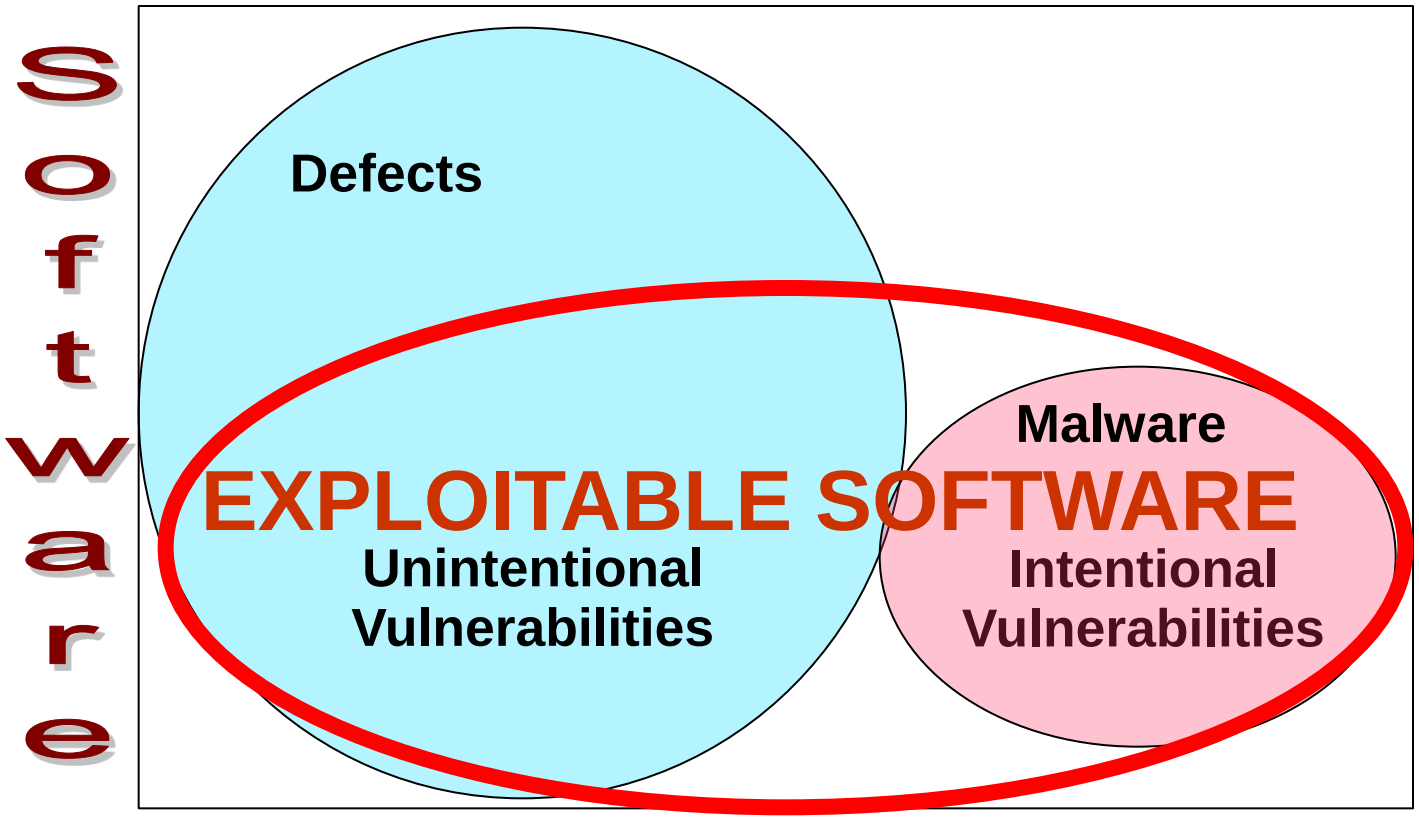
- Software is the core constituent of modern products and services – it enables functionality and business operations
- Dramatic increase in mission risk due to increasing:
  - Software dependence and system interdependence (weakest link syndrome)
  - Software Size & Complexity (obscures intent and precludes 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

Homeland Security

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

Software Assurance Addresses Exploitable Software:
Outcomes of non-secure practices and/or malicious intent

Exploitation potential of vulnerability is independent of "intent"



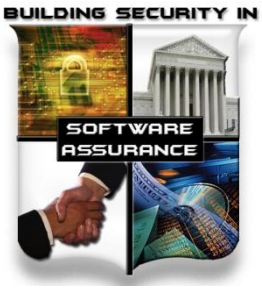
'High quality' can reduce security flaws attributable to defects; yet traditional S/W quality assurance does not address intentional malicious behavior in software

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

Homeland Security

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

Security-Enhanced Capabilities:
Mitigating Risks to the Enterprise



- With today's global software supply chain, Software Engineering, Quality Assurance, Testing and Project Management must explicitly address security risks posed by exploitable software.
  - Traditional processes do not explicitly address software-related security risks that can be passed from projects to using organizations.
- Mitigating Supply Chain Risks requires an understanding and management of Suppliers' Capabilities, Products and Services
  - Enterprise risks stemming from supply chain are influenced by suppliers and acquisition projects (including procurement, SwEng, QA, & testing).
  - IT/Software Assurance processes/practices span development/acquisition.
  - Derived (non-explicit) security requirements should be elicited/considered.
- More comprehensive diagnostic capabilities and standards are needed to support processes and provide transparency for more informed decision-making for mitigating risks to the enterprise

Homeland Security

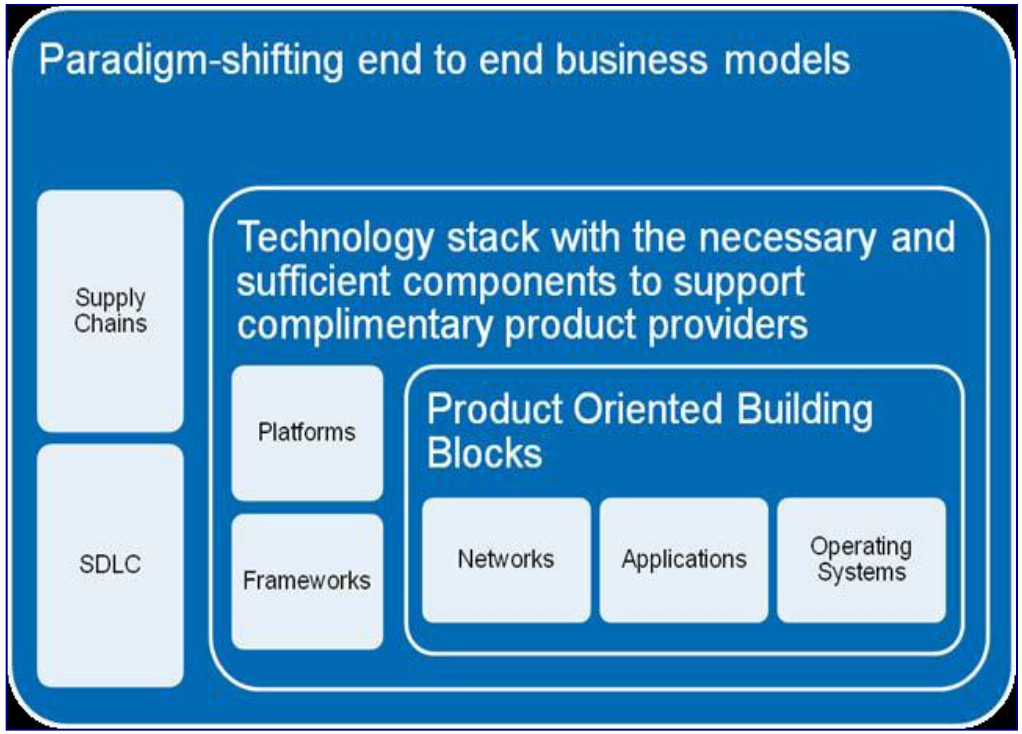
Free resources are available to assist personnel in security-enhancing contracting, outsourcing and development activities (see https://buildsecurityin.us-cert.gov)

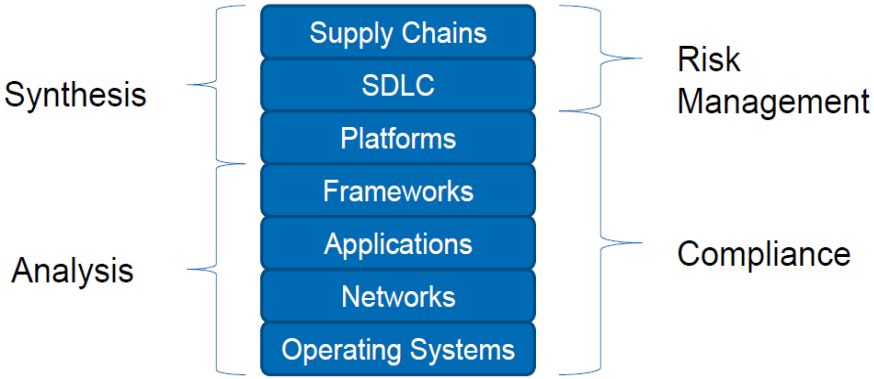
IT/software security risk landscape is a convergence between “defense in depth” and “defense in breadth”

Enterprise Risk Management and Governance are security motivators

Acquisition could be considered the beginning of the lifecycle; not development

> “In the digital age, sovereignty is demarcated not by territorial frontiers but by supply chains.”
>
> – Dan Geer, CISO In-Q-Tel

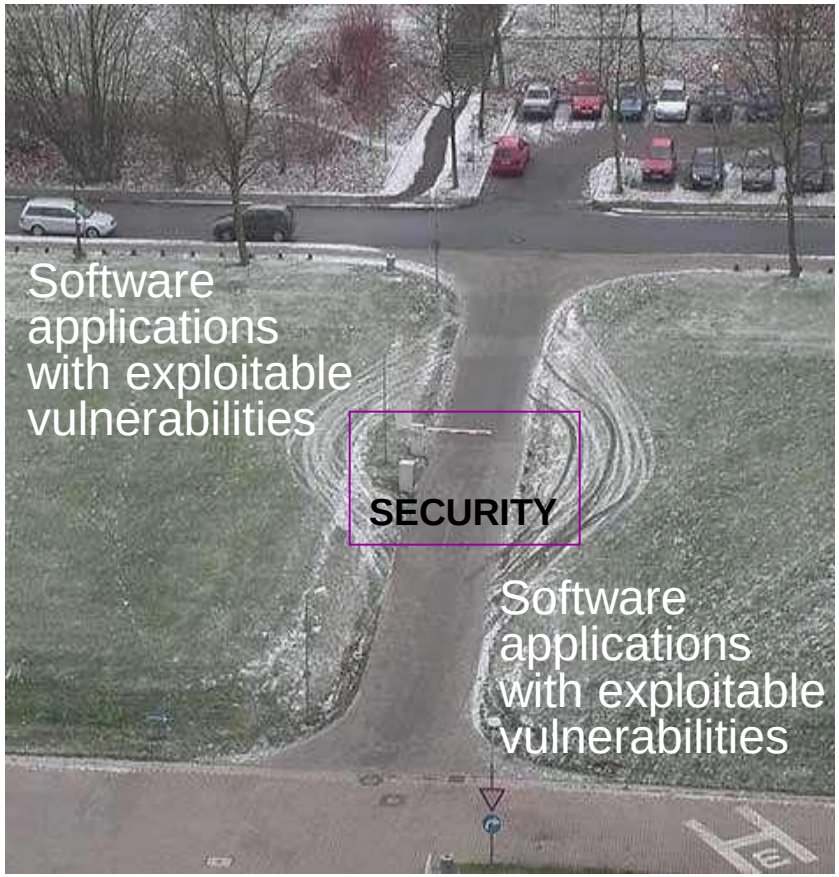




Software Assurance provides a focus for:
-- Secure Software Components,
-- Security in the Software Life Cycle and
-- Software Supply Chain Risk Management

Security is a Requisite Quality Attribute:
Vulnerable Software Enables Exploitation

- Rather than attempt to break or defeat network or system security, hackers are opting to target application software to circumvent security controls.
  - **75% of hacks occurred at application level**
    - "90% of software attacks were aimed at application layer" (Gartner & Symantec, June 2006)
  - most exploitable software vulnerabilities are attributable to non-secure coding practices (and not identified in testing).
- Functional correctness must be exhibited even when software is subjected to abnormal and hostile conditions



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

Homeland Security

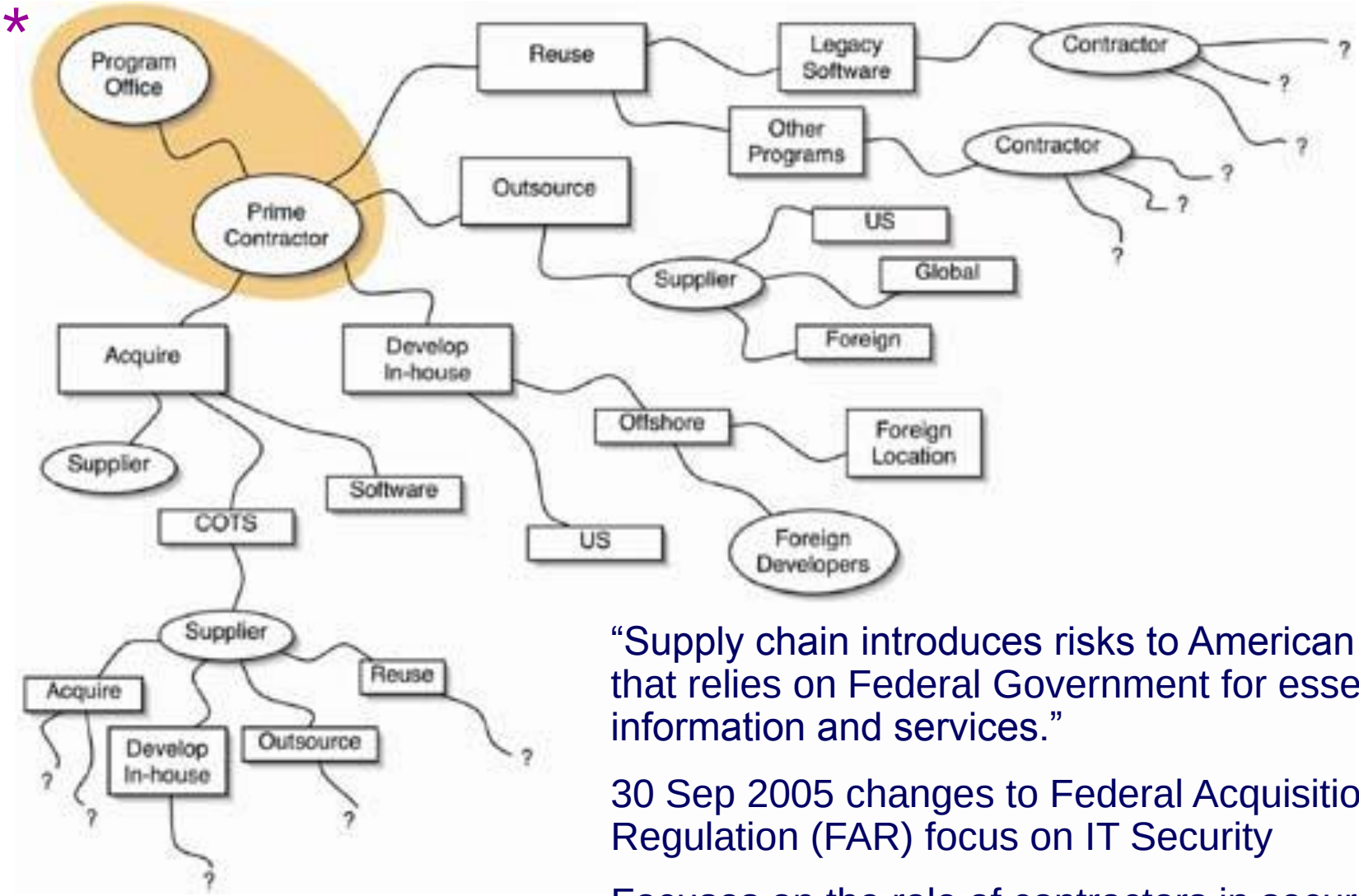
DHS NCSD Software Assurance (SwA) Program

Through public-private collaboration promotes security and resilience of software throughout the lifecycle; focused on reducing exploitable software weaknesses and addressing means to improve capabilities that routinely develop, acquire, and deploy resilient software products. Collaboratively advancing software-relevant rating schemes

- **Serves as a focal point for interagency public-private collaboration to enhance development and acquisition processes and capability benchmarking to address software security needs.**
  - Hosts interagency Software Assurance Forums, Working Groups and training to provide public-private collaboration in advancing software security and providing publicly available resources.
  - Provides collaboratively developed, peer-reviewed information resources on Software Assurance, via journals, guides & on-line resources suitable for use in education, training, and process improvement.
  - Provides input and criteria for leveraging international standards and maturity models used for process improvement and capability benchmarking of software suppliers and acquisition organizations.

- **Enables software security automation and measurement capabilities through use of common indexing and reporting capabilities for malware, exploitable software weaknesses, and common attacks which target software.**
  - Collaborates with the National Institute of Standards and Technology, international standards organizations, and tool vendors to create standards, metrics and certification mechanisms from which tools can be qualified for software security verification.
  - Manages programs for Malware Attribute Enumeration Classification (MAEC), Common Weakness Enumeration (CWE), and Common Attack Pattern Enumeration and Classification (CAPEC).
  - Manages programs for Common Vulnerabilities & Exposures (CVE) and Open Vulnerability & Assessment Language (OVAL) that provide information feeds for Security Content Automation Protocol (SCAP), vulnerability databases, and security/threat alerts from many organizations

*



"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

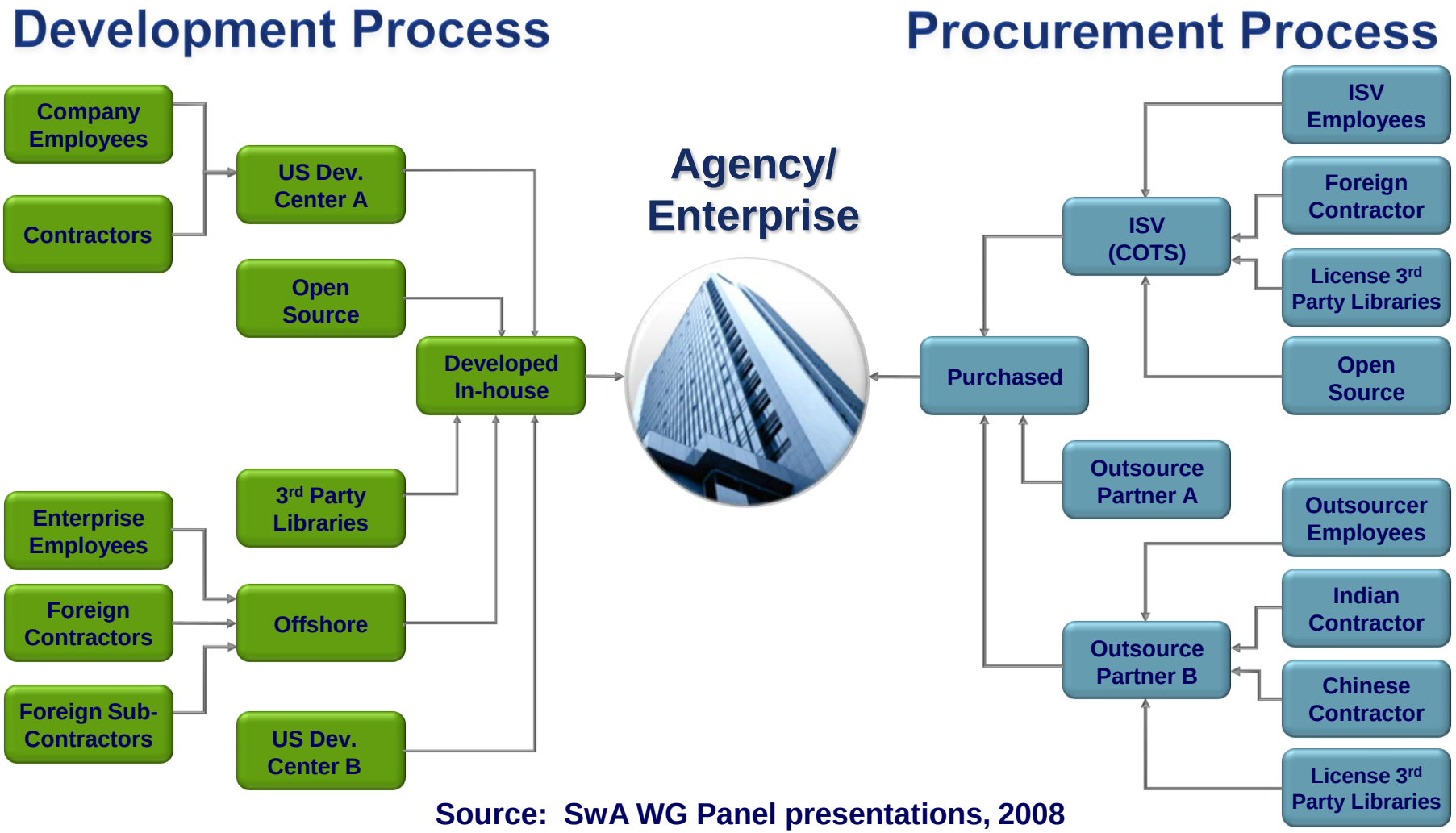
Focuses on the role of contractors in security as Federal agencies outsource various IT functions.

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"

Enterprise Processes for deploying capabilities: Increasingly Distributed and Complex

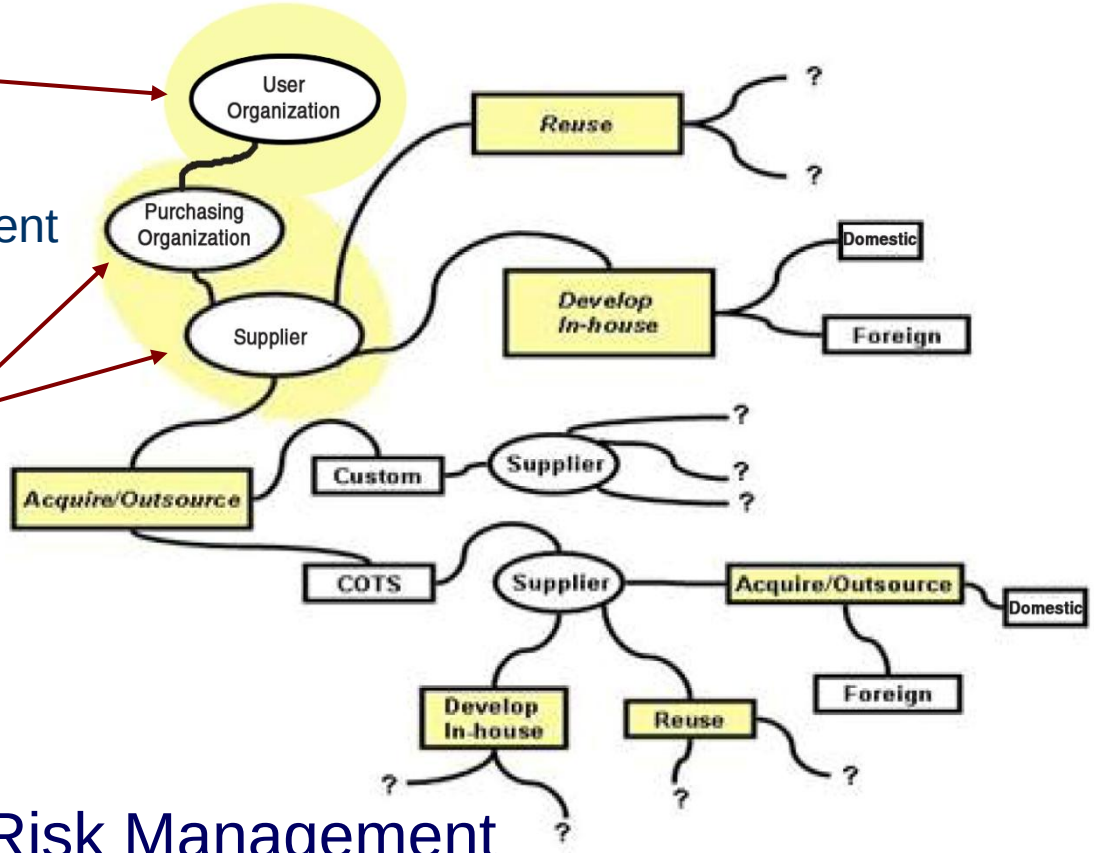
New Considerations for Quality & Security



Source: SwA WG Panel presentations, 2008

Risk Management (Enterprise <=> Project):
Shared Processes & Practices // Different Focuses

- Enterprise-Level:
  - Regulatory compliance
  - Changing threat environment
  - Business Case
- Program/Project-Level:
  - Cost
  - Schedule
  - Performance



Software Supply Chain Risk Management traverses enterprise and program/project interests

Homeland Security

The New Issue is Virtual Security

- In addition to physical security, we now worry about cyber risks:
  - Theft of intellectual property
  - Fake or counterfeit products
  - Import/export of strong encryption
  - IT/software with deliberately embedded malicious functionality
    - Logic bombs and self-modifying code
    - Other "added features" like key loggers
    - Deliberately hidden back doors for unauthorized remote access
  - Exploitable IT/software from suppliers with poor security practices
    - Failure to use manufacturing processes/capabilities to design and build secure products (no malicious intent) in delivering exploitable products
    - Resuppliers (VARs, integrators, and service providers) often lack incentives and capabilities to adequately check content of sub-contracted and outsourced IT/software products

- IT/software security laws, policies, & standards are immature

Homeland Security

Adopted in part from Marcus H. Sachs, Verizon, *"Supply Chain Risk Management: Can we Secure the IT Supply Chain in the Age of Globalization?" Software Assurance Forum, 15 Oct 2008*

Need for Rating Schemes

- Rating of Software products:
  - Supported by automation
  - Standards-based
  - Rules for aggregation and scaling
  - Verifiable by independent third parties
  - Labeling to support various needs (eg., security, dependability, etc)
  - Meaningful and economical for consumers and suppliers

Collaborate with "Security Facts" labeling efforts

- Rating of Suppliers providing software products and services
  - Standards-based or model-based frameworks to support process improvement and enable benchmarking of organizational capabilities
  - Credential programs for professionals involved in software lifecycle activities and decisions

SwA Collaboration for Content & Peer Review

BSI https://buildsecurityin.us-cert.gov focuses on making Software Security a normal part of Software Engineering

SwA Community Resources and Information Clearinghouse (CRIC)

https://buildsecurityin.us-cert.gov/swa/ focuses on all contributing disciplines, practices and methodologies that advance risk mitigation efforts to enable greater resilience of software/cyber assets.

The SwA CRIC provides a primary resource for SwA Working Groups.

Where applicable, SwA CRIC & BSI provide relevant links to each other.

Software Assurance (SwA) Pocket Guide Series

SwA in Acquisition & Outsourcing

- Software Assurance in Acquisition and Contract Language
- Software Supply Chain Risk Management and Due-Diligence

SwA in Development

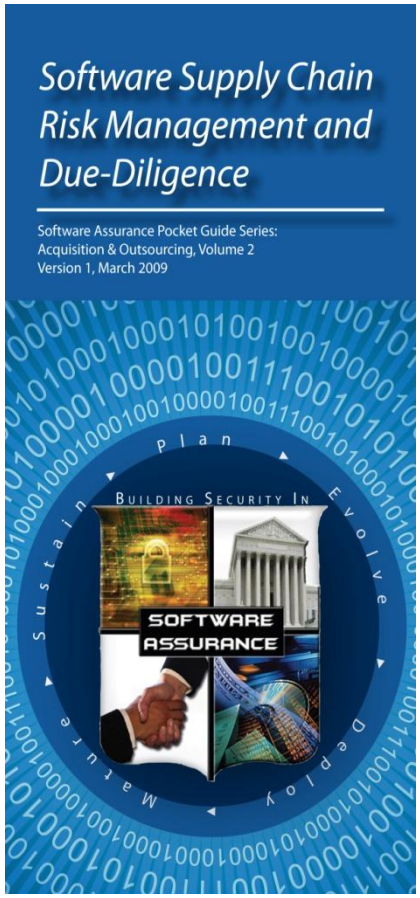
- Integrating Security into the Software Development Life Cycle
- Key Practices for Mitigating the Most Egregious Exploitable Software Weaknesses
- Risk-based Software Security Testing
- Requirements and Analysis for Secure Software
- Architecture and Design Considerations for Secure Software
- Secure Coding and Software Construction
- Security Considerations for Technologies, Methodologies & Languages

SwA Life Cycle Support

- SwA in Education, Training and Certification
- Secure Software Distribution, Deployment, and Operations
- Code Transparency & Software Labels
- Assurance Case Management
- Secure Software Environment and Assurance EcoSystem

SwA Measurement and Information Needs

- Making Software Security Measurable
- Practical Measurement Framework for SwA and InfoSec
- SwA Business Case and Return on Investment



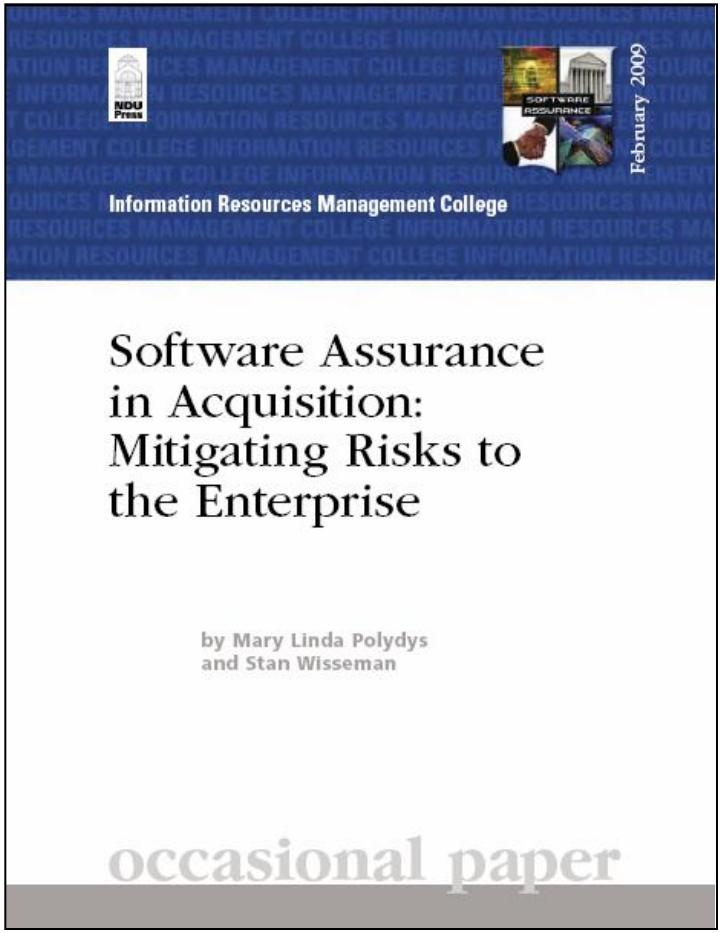
SwA Pocket Guides and SwA-related documents are collaboratively developed with peer review; they are subject to update and are freely available for download via the DHS Software Assurance Community Resources and Information Clearinghouse at https://buildsecurityin.us-cert.gov/swa (see SwA Resources)

SwA Acquisition & Outsourcing Handbook

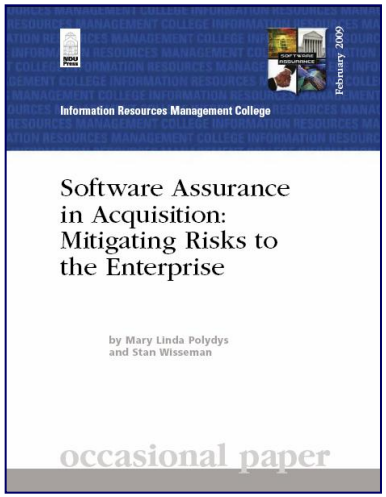
"Software Assurance in Acquisition:
Mitigating Risks to the Enterprise"

Version 1.0, Oct 2008, available for community use

published by National Defense University Press, Feb 2009



SwA Acquisition & Outsourcing Handbook



Software Supply Chain Risk Management and Due-Diligence -- Table 1 –SwA Concern Categories		
SwA Concern Categories	**Risks**	**Purpose for Questions**
Software History and Licensing **Development Process Management** **Software Security Training and Awareness** **Planning and Requirements** **Architecture and Design** **Software Development** **Built-in Software Defenses** **Component Assembly** **Testing** **Software Manufacture and Packaging** **Installation** **Assurance Claims and Evidence** **Support** **Software Change Management** **Timeliness of Vulnerability Mitigation** **Individual Malicious Behavior** **Security "Track Record"** **Financial History and Status** **Organizational History** **Foreign Interests and Influences** **Service Confidentiality Policies** **Operating Environment for Services** **Security Services and Monitoring**		

Software Supply Chain Risk Management and Due-Diligence -- Table 1 –SwA Concern Categories

SwA Concern Categories	Risks	Purpose for Questions
Individual Malicious Behavior	A developer purposely inserts malicious code, and supplier lacks procedures to mitigate risks from insider threats within the supply chain.	To determine whether the supplier has and enforces policies to minimize individual malicious behavior.
Security "Track Record"	A software supplier that is unresponsive to known software vulnerabilities may not mitigate/patch vulnerabilities in a timely manner.	To establish insight into whether the supplier places a high priority on security issues and will be responsive to vulnerabilities they will need to mitigate.
Financial History and Status	A software supplier that goes out of business will be unable to provide support or mitigate product defects and vulnerabilities.	To identify documented financial conditions or actions of the supplier that may impact its viability and stability, such as mergers, sell-offs, lawsuits, and financial losses.
Organizational History	There may be conflicting circumstances or competing interests within the organization that may lead to increased risk in the software development.	To understand the supplier's organizational background, roles, and relationships that might have an impact on supporting the software.
Foreign Interests and Influences	There may be controlling foreign interests (among organization officers or from countries) with malicious intent to the users' country or organization planning to use the software.	To help identify supplier companies that may have individuals with competing interests or malicious intent to a domestic buyer/user.
Service Confidentiality Policies	Without policies to enforce client data confidentiality/ privacy, acquirer's data could be at risk without service supplier liability.	To determine the service provider's confidentiality and privacy policies and ensure their enforcement.
Operating Environment for Services	Operating environment for the services may not be hardened or otherwise secure.	To understand the controls the supplier has established to operate the software securely.
Security Services and Monitoring	Insufficient security monitoring may allow attacks to impact services.	To ensure software and its operating environment are regularly reviewed for adherence to SwA requirements through periodic testing and evaluation.

Table 2- Questions for COTS (Proprietary & Open Source), GOTS, and Custom Software					
No.	Question	COTS Proprietary	COTS Open-Source	GOTS	Custom
11	Does the license/contract restrict the licensee from discovering flaws or disclosing details about software defects or weaknesses with others (e.g., is there a “gag rule” or limits on sharing information about discovered flaws)?	✓			✓
12	Does the license/contract restrict communications or limit the licensee in any potential communication with third-party advisors about provisions for support (e.g., is there a “gag rule” or limits placed on the licensee that affect ability to discuss contractual terms or breaches) regarding the licensed or contracted product or service?	✓			✓
13	Does software have a positive reputation? Does software have a positive reputation relative to security? Are there reviews that recommend it?	✓	✓		
14	Is the level of security where the software was developed the same as where the software will operate?			✓	✓
Development Process Management					
15	What are the processes (e.g., ISO 9000, CMMI, etc.), methods, tools (e.g., IDEs, compilers), techniques, etc. used to produce and transform the software (brief summary response)?	✓		✓	✓
16	What security measurement practices and data does the company use to assist product planning?	✓			✓
17	Is software assurance considered in all phases of development? Explain.	✓		✓	✓
18	How is software risk managed? Are anticipated threats identified, assessed, and prioritized?	✓		✓	✓

Table 1 –SwA Concern Categories -- (with interests relevant to security and privacy)		
SwA Concern Categories	**Risks**	**Purpose for Questions**
Service Confidentiality Policies	Without policies to enforce client data confidentiality/ privacy, acquirer's data could be at risk without service supplier liability.	To determine the service provider's confidentiality and privacy policies and ensure their enforcement.

Table 3 - Questions for Hosted Applications	
No.	Questions
Service Confidentiality Policies	
1	What are the customer confidentiality policies? How are they enforced?
2	What are the customer privacy policies? How are they enforced?
3	What are the policies and procedures used to protect sensitive information from unauthorized access? How are the policies enforced?
4	What are the set of controls to ensure separation of data and security information between different customers that are physically located in the same data center? On the same host server?
Operating Environment for Services	
5	Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all registry settings?
7	What are the data backup policies and procedures? How frequently are the backup procedures verified?
11	What are the agents or scripts executing on servers of hosted applications? Are there procedures for reviewing the security of these scripts or agents?
12	What are the procedures and policies used to approve, grant, monitor and revoke access to the servers? Are audit logs maintained?
13	What are the procedures and policies for handling and destroying sensitive data on electronic and printed media?
15	What are the procedures used to approve, grant, monitor, and revoke file permissions for production data and executable code?

More Due-Diligence Questions Relevant to Acquisition & Outsourcing

- **Relevant to deliberate actions that are controllable and preventable by developers that have security implications**
  - **"Were any compiler warnings disabled for the software being delivered?"**
- **Relevant to hosted applications and services**
  - **Cloud computing, "XXXX_as a Service," SOA,**

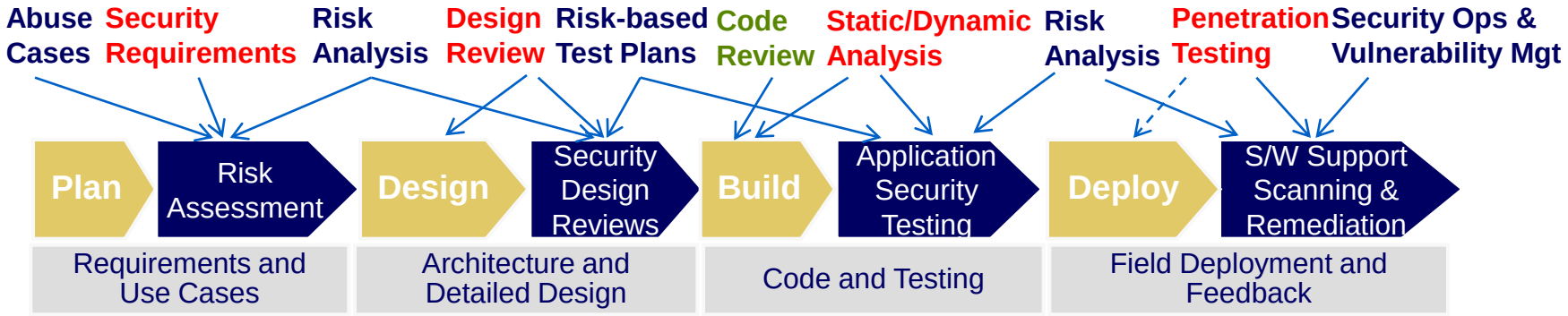
Seeking more examples from "security aware" community

Security-Enhanced Process Improvements

Organizations that provide security engineering & risk-based analysis throughout the lifecycle will have more resilient software products / systems.

"Build Security In" throughout the lifecycle

Attack Modeling	Secure S/W Requirements Engineering	Secure Design Principles & Practices	Secure Programming Practices	Test / Validation of Security & Resilience	Secure Distribution/ Deployment	Documentation for Secure Use & Configuration



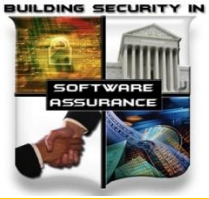
Organizational Process Assets cover: governance, policies, standards, training, tailoring guidelines

- Leverage Software Assurance resources (freely available) to incorporate in training & awareness
- Modify SDLC to incorporate security processes and tools (should be done in phases by practitioners to determine best integration points)
- Avoid drastic changes to existing development environment and allow for time to change culture and processes
- Make the business case and balance the benefits
- Retain upper management sponsorship and commitment to producing secure software.

Homeland Security

* Adopted in part from "Software Assurance: Mitigating Supply Chain Risks" (DHS NCSD SwA); "What to Test from a Security Perspective for the QA Professional" (Cigital) and "Neutralizing the Threat: A Case Study in Enterprise-wide Application Security Deployments" (Fortify Software & Accenture Security Technology Consulting)

Build Security In the SDLC



- Adding security practices throughout the SDLC establishes a software life cycle process that codifies both caution and intention.
- Key elements of a secure software life cycle process are:
  1. Security criteria in all software life cycle checkpoints (at entry & exit of a life cycle phase)
  2. Adherence to secure software principles and practices
  3. Adequate requirements, architecture, and design to address software security
  4. Secure coding practices with secure software integration/assembly practices
  5. Security testing practices that focus on verifying S/W dependability, trustworthiness, & resiliency
  6. Secure distribution and deployment practices and mechanisms
  7. Secure sustainment practices
  8. Supportive security tools (providing static & dynamic analysis) for developers and testers
  9. Secure software configuration management systems and processes
  10. Security risk analysis throughout the lifecycle
- Key people for producing secure software are:
  1. Security-knowledgeable software professionals
  2. Security-aware project management
  3. Upper management commitment to production of secure software

Homeland Security

Adopted from **Build Security In web site "Introduction to Software Security"** which adapted or excerpted from *Enhancing the Development Life Cycle to Produce Secure Software: A Reference Guidebook on Software Assurance* [DHS/DACS 08].

Life-Cycle Standards View Categories (ISO/IEC 15288 and 12207)

Organization

Governance Processes

Strategy and policy

Enterprise risk management
- Compliance
- Business case

Supply Chain Management

Project-Enabling Processes

Life Cycle Model Management

Infrastructure Management
- SwA ecosystem
- Enumerations, languages, and repositories

Project Portfolio Management

Human Resource Management
- SwA education
- SwA certification and training
- Recruitment

Quality Management

Agreement Processes

Acquisition
- Outsourcing
- Agreements
- Risk-based due diligence
- Supplier assessment

Supply

Project

Project Management Processes

Project Planning

Project Assessment and Control
- Assurance case management

Project Support Processes

Decision Management

Risk Management
- Threat Assessment

Configuration Management

Information Management

Measurement

Engineering

Technical Processes

Stakeholder Requirements Definition

Requirements Analysis
•Attack modeling (misuse and abuse cases)
•Data and information classification
•Risk-based derived requirements
•Sw security requirements

Architectural Design
•Secure Sw architectural design
•Risk-based architectural analysis
•Secure Sw detailed design and analysis

Implementation
•Secure coding and Sw construction
•Security code review and static analysis
•Formal methods

Integration
•Sw component integration
•Risk analysis of Sw reuse components

Verification & Validation
•Risk-based test planning
•Security-enhanced test and evaluation
- Dynamic and static code analysis
- Penetration testing

•Independent test and certification

Transition
•Secure distribution and delivery
•Secure software environment (secure configuration, application monitoring, code signing, etc)

Operations and Sustainment

Operation
- Incident handling and response

Maintenance
- Defect tracking and remediation
- Vulnerability and patch management
- Version control and management

Disposal

Software Reuse Processes

Domain Engineering

Reuse Asset Management

Reuse Program Management

Software Support Processes

Sw Documentation Management

Sw Quality Assurance

Sw Configuration Management

Sw Verification & Sw Validation

Sw Review

Sw Audit

Sw Problem Resolution

CWE List
Full Dictionary View
Development View
Research View
Reports
About
Sources
Process
Documents
Community
Related Activities
Discussion List
Research
CWE/SANS Top 25
CWSS
News
Calendar
Free Newsletter
Compatibility
Program
Requirements
Declarations
Make a Declaration
Contact Us
Search the Site

2010 CWE/SANS Top 25 Most Dangerous Software Errors

http://cwe.mitre.org/top25/

Document version: 1.06 (pdf)

Date: September 27, 2010

Project Coordinators:

Bob Martin (MITRE)
Mason Brown (SANS)
Alan Paller (SANS)
Dennis Kirby (SANS)

Document Editor:

Steve Christey (MITRE)

Section Contents
CWE/SANS Top 25
Contributors
Supporting Quotes
Monster Mitigations
Focus Profiles
On the Cusp
Documents & Podcasts
Training Materials
Top 25 FAQ
Top 25 Process
Change Log
SANS News Release

Section Archives
2009 CWE/SANS Top 25
Supporting Quotes
Contributors
On The Cusp
Change Log

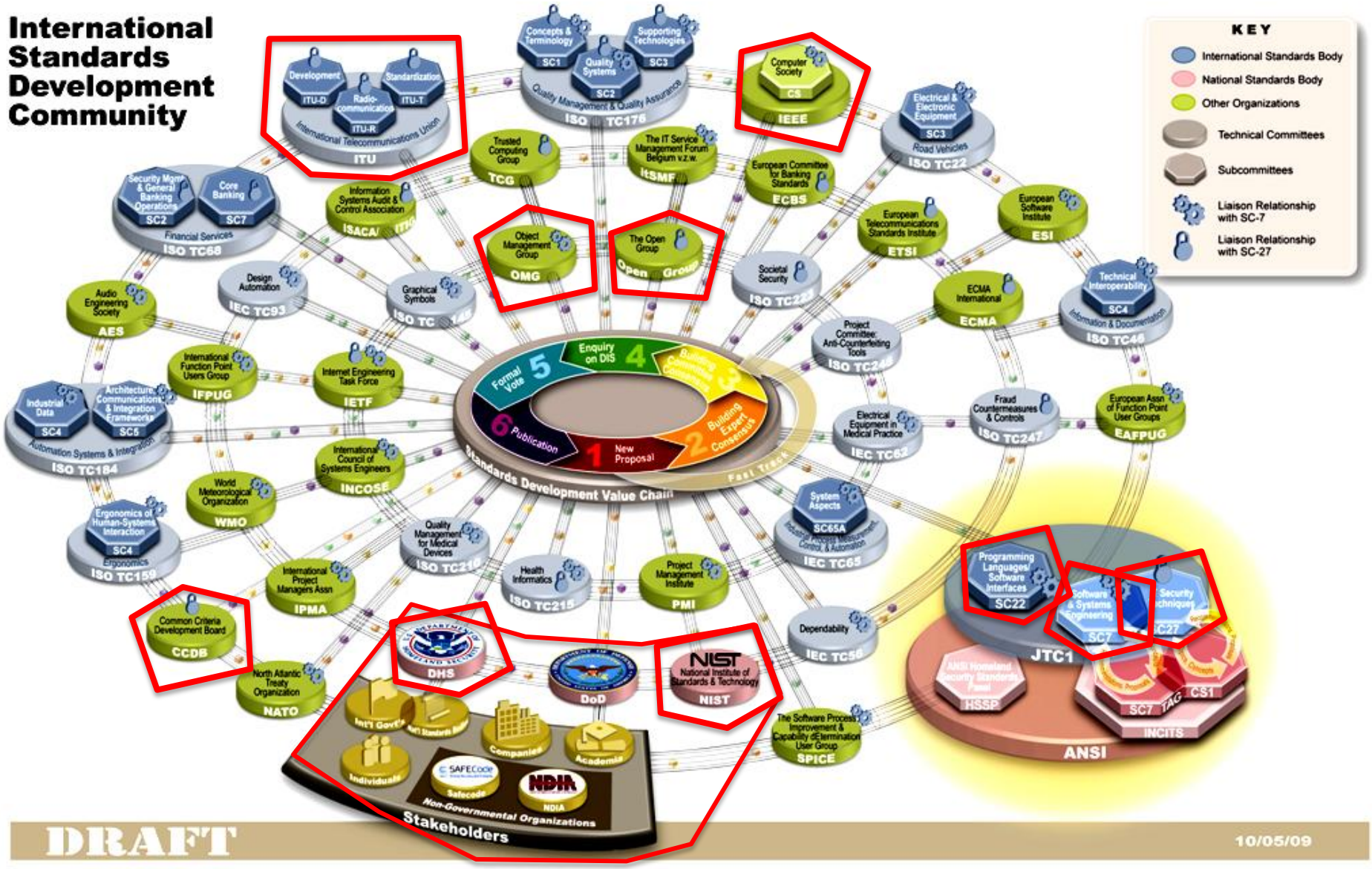
Introduction

The 2010 CWE/SANS Top 25 Most Dangerous Software Errors is a list of the most widespread and critical programming errors that can lead to serious software vulnerabilities. They are often easy to find, and easy to exploit. They are dangerous because they will frequently allow attackers to completely take over the software, steal data, or prevent the software from working at all.

The Top 25 list is a tool for education and awareness to help programmers to prevent the kinds of vulnerabilities that plague the software industry, by identifying and avoiding all-too-common mistakes that occur before software is even shipped. Software customers can use the same list to help them to ask for more secure software. Researchers in software security can use the Top 25 to focus on a narrow but important subset of all known security weaknesses. Finally, software managers and CIOs can use the Top 25 list as a measuring stick of progress in their efforts to secure their software.

The list is the result of collaboration between the SANS Institute, MITRE, and many top software security experts in the US and Europe. It leverages experiences in the development of the SANS Top 20 attack vectors (http://www.sans.org/top20/) and MITRE's Common Weakness Enumeration (CWE) (http://cwe.mitre.org/). MITRE maintains the CWE web site, with the support of the US Department of Homeland Security's National Cyber Security Division, presenting detailed descriptions of the top 25 programming errors along with authoritative guidance for mitigating and avoiding them. The CWE site contains data on more than 800 programming errors, design errors, and architecture errors that can lead to exploitable

We are engaged with many parts of the Community for Software Assurance-related standardization



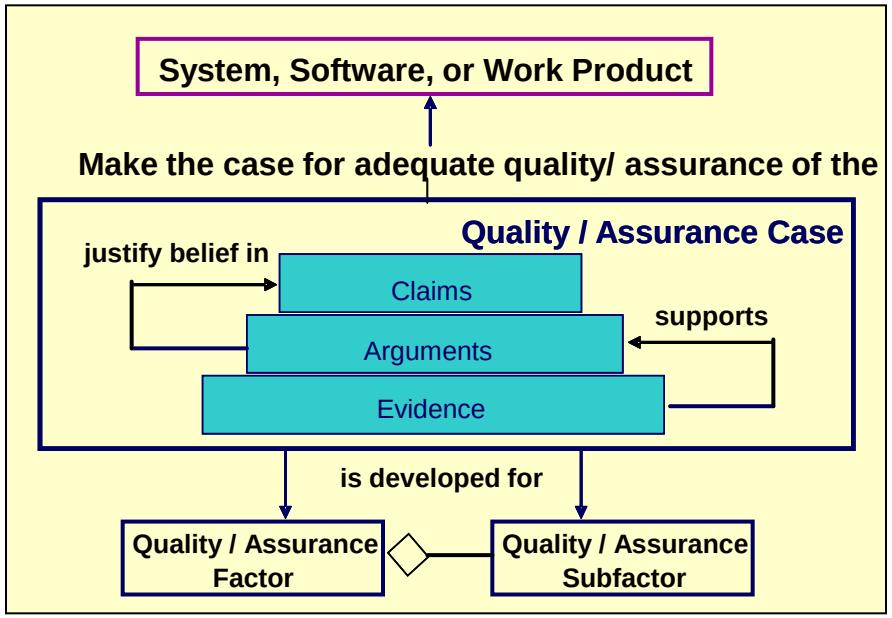
ISO/IEC JTC1

- **SC22: ISO/IEC Technical Report (TR) 24772 Information technology -- Programming languages -- Guidance to avoiding vulnerabilities in programming languages through language selection and use.**
  - This technical report was reviewed and approved by the project editor, then published in early October.
  - As published, the document includes language-independent summaries of nearly 70 classes of vulnerabilities.
  - The working group is already drafting the 2nd Edition of the report which will add information specific to individual programming languages.

- **SC7: ISO/IEC 15026-2, Software Assurance Case has entered Final Draft International Standard (FDIS) ballot; the final ISO/IEC ballot will complete in December 2010.**
  - Upon completion, it will be submitted for its final IEEE recirculation.
  - It is reasonable to anticipate publication of the standard, by both ISO/IEC and IEEE, in spring 2011.

ISO/IEC/IEEE 15026 Assurance Case

- **Set of structured assurance claims, supported by evidence and reasoning (arguments), 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

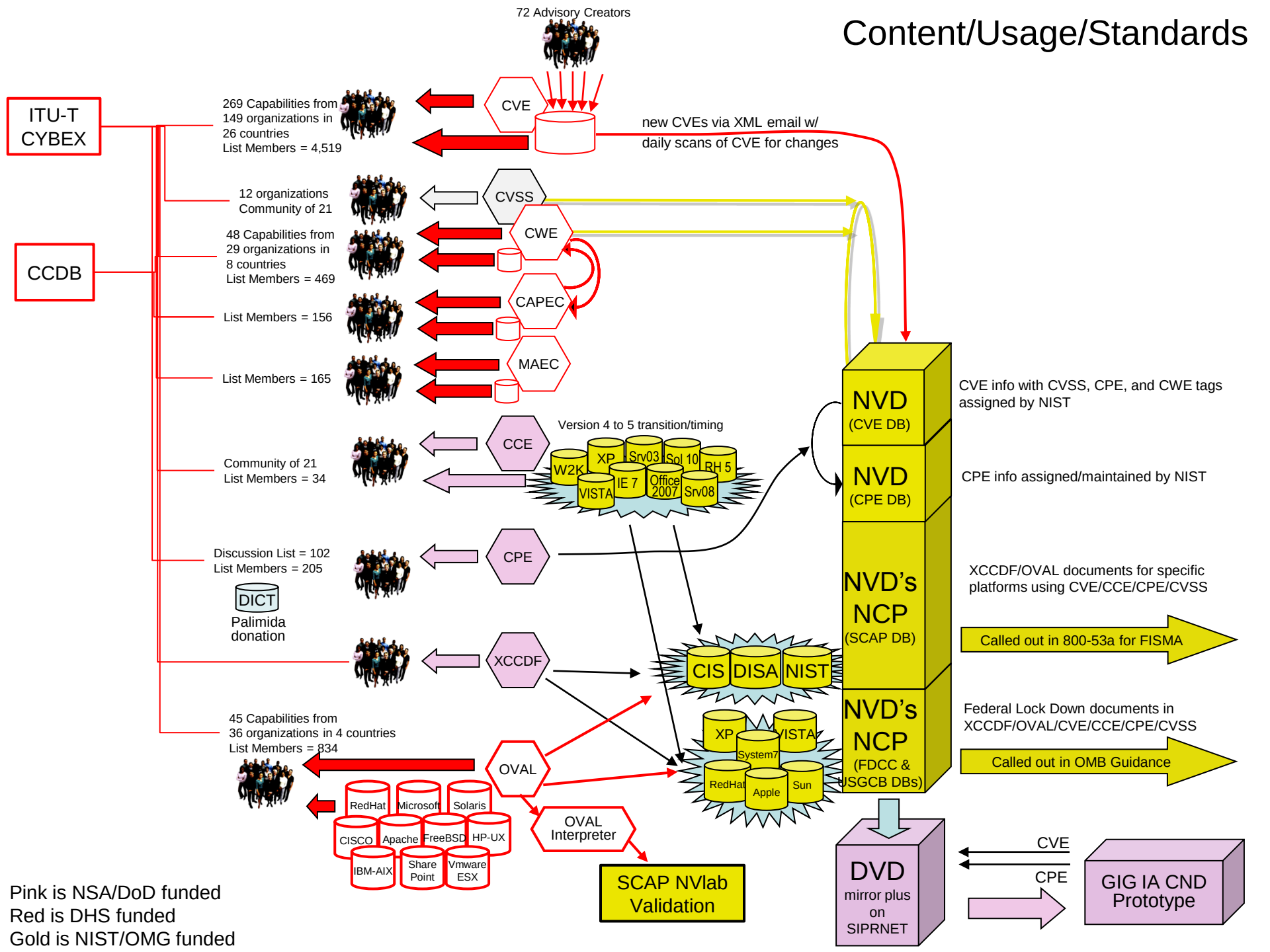


- **Sub-parts**
  - A high level summary
  - Justification that product or service is acceptably safe, secure, or dependable
  - Rationale for claiming a specified level of safety and security
  - Conformance with relevant standards & regulatory requirements
  - The configuration baseline
  - Identified hazards and threats and residual risk of each hazard / threat
  - Operational & support assumptions

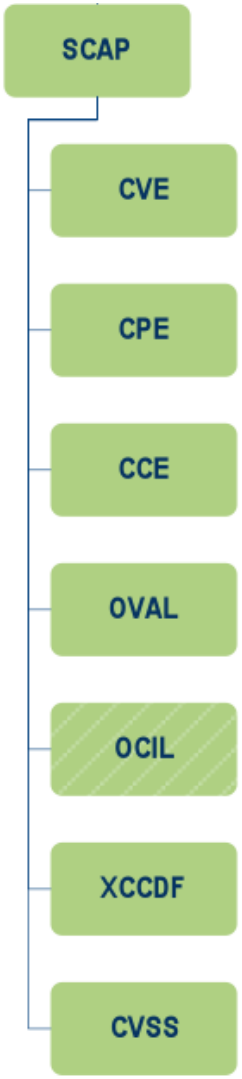
Attributes

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

Content/Usage/Standards



Pink is NSA/DoD funded
Red is DHS funded
Gold is NIST/OMG funded



SCAP 1.1 uses the following specifications:

- Extensible Configuration Checklist Description Format (XCCDF) 1.1.4, a language for authoring security checklists/benchmarks and for reporting results of checklist evaluation [QUI08]
- Open Vulnerability and Assessment Language (OVAL) 5.6, a language for representing system configuration information, assessing machine state, and reporting assessment results
- Open Checklist Interactive Language (OCIL) 2.0, a language for representing security checks that requires human feedback
- Common Platform Enumeration (CPE) 2.2, a nomenclature and dictionary of hardware, operating systems, and applications [BUT09]
- Common Configuration Enumeration (CCE) 5, a nomenclature and
  configurations
- Common Vulnerabilities and Exposures (CVE), a nomenclature an
  software flaws[9]
- Common Vulnerability Scoring System (CVSS) 2.0, an open speci
  severity of software flaw vulnerabilities [MEL07].

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-126
Revision 1 (DRAFT)

The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1 (DRAFT)

Recommendations of the National Institute of Standards and Technology

Stephen Quinn
David Waltermire
Christopher Johnson
Karen Scarfone
John Banghart

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-126
Revision 1 (DRAFT)

The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1 (DRAFT)

Recommendations of the National Institute of Standards and Technology

Stephen Quinn
David Waltermire
Christopher Johnson
Karen Scarfone
John Banghart

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-126
Revision 1 (DRAFT)

The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1 (DRAFT)

Recommendations of the National Institute of Standards and Technology

Stephen Quinn
David Waltermire
Christopher Johnson
Karen Scarfone
John Banghart

SwAAP

CWE

CAPEC

MAEC

CWSS

OMG SAEM

OMG ARG

SAFES

"Food Label"

OMG SMM

ISO 15026

OMG KDM

OMG ASTM

Software Assurance Automation Protocol (SwAAP)

- For measuring & enumerating software weaknesses and the assurance cases.

Common Weakness Enumeration (CWE),

Common Attack Pattern Enumeration & Classification (CAPEC),

Malware Attribute Enumeration & Characterization (MAEC),

Common Weakness Scoring System (CWSS),

Software Assurance Findings Expression Schema (SAFES),

NIST SAMATE's "Software Transparency Label",

ISO/IEC 15026 "Assurance Case" (ISO 15026),

OMG Software Assurance Evidence Metamodel (OMG SAEM),

OMG Argumentation Metamodel (OMG ARG),

OMG Structured Metrics Metamodel (OMG SMM),

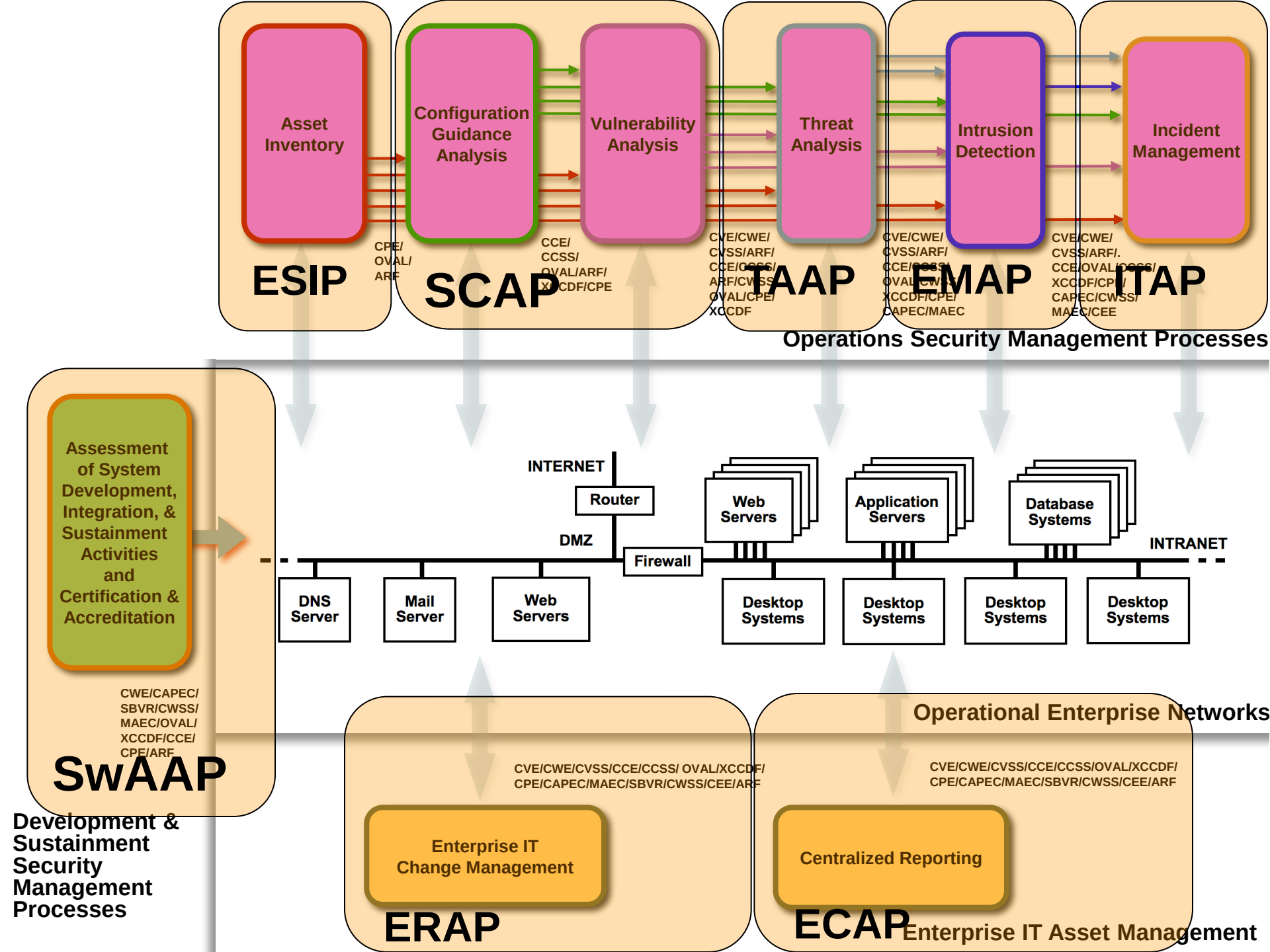
OMG Knowledge Discovery Metamodel (OMG KDM),

OMG Abstract Syntax Tree Metamodel (OMG ASTM)

- plus SCAP to capture "accredited" system CPEs and CCE settings?
- OVAL checks for capturing "finger print" of software applications to address supply-chain risk measurement?

“Other” Automation Protocols (“O”AP)

- Event Management Automation Protocol (EMAP)
  - For reporting of security events.
  - Uses Common Event Expression (CEE), Malware Attribute Enumeration & Characterization (MAEC), CAPEC, etc.
- Enterprise Remediation Automation Protocol (ERAP)
  - For automated remediation of mis-configuration & missing patches.
  - Uses Common Remediation Enumeration (CRE) and Extended Remediation Information (ERI).
- Enterprise Compliance Automation Protocol (ECAP)
  - For reporting configuration compliance.
  - Uses Asset Reporting Format (ARF), Open Checklist Reporting Language (OCRL), etc.
- Enterprise System Information Protocol (ESIP)
  - For reporting of asset inventory information.
  - Uses …..
- Threat Analysis Automation Protocol (TAAP)
  - For analyzing threats and security risks.
  - Uses….
- Incident Tracking and Assessment Protocol (ITAP)
  - For supporting incident management and response.
  - Uses IODEF, etc


Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
CPE/ OVAL/ ARF
CCE/ CCSS/ OVAL/ARF/ XCCDF/CPE
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ ARF/CWSS/ OVAL/CPE/ XCCDF
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ OVAL/CWSS/ XCCDF/CPE/ CAPEC/MAEC
CVE/CWE/ CVSS/ARF/. CCE/OVAL/CCSS/ XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE
ESIP
SCAP
TAAP
EMAP
ITAP
Operations Security Management Processes
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
CWE/CAPEC/ SBVR/CWSS/ MAEC/OVAL/ XCCDF/CCE/ CPE/ARF
SwAAP
INTERNET
Router
DMZ
Firewall
Web Servers
Application Servers
Database Systems
INTRANET
DNS Server
Mail Server
Web Servers
Desktop Systems
Desktop Systems
Desktop Systems
Desktop Systems
Operational Enterprise Networks
CVE/CWE/CVSS/CCE/CCSS/ OVAL/XCCDF/ CPE/CAPEC/MAEC/SBVR/CWSS/CEE/ARF
CVE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/SBVR/CWSS/CEE/ARF
Development & Sustainment Security Management Processes
Enterprise IT Change Management
ERAP
Centralized Reporting
ECAP
Enterprise IT Asset Management

Software Assurance (SwA) – Security Automation

- Security Content Automation Protocol (SCAP)
- Software Assurance Automation Protocol (SwAAP)
- Enterprise System Information Protocol (ESIP)
- Enterprise Remediation Automation Protocol (ERAP)
- Enterprise Compliance Automation Protocol (ECAP)
- Event Management Automation Protocol (EMAP)
- Incident Tracking and Assessment Protocol (ITAP)
- Threat Analysis Automation Protocol (TAAP)

Use Cases for Enterprise IT Security

	SCAP	SwAAP	ESIP	ERAP	ECAP	EMAP	ITAP	TAAP
CVE	X						X	X
OVAL	X						X	X
XCCDF	X							
CVRF	X							
OCIL	X						X	
CPE	X		X				X	X
CCE	X							X
CWE		X						X
CAPEC		X				X	X	X
MAEC		X				X	X	X

	SCAP	SwA AP	ESIP	ERAP	ECAP	EMAP	ITAP	TAAP
CEE						X	X	
CRE				X				
ERI				X				
ARF					X			
OCRL					X			
IODEF							X	
NIEM							X	
CYBEX							X	

Software Assurance Ecosystem: The Formal Framework

The value of formalization extends beyond software systems to include related software system process, people and documentation

Process Docs & Artifacts

Requirements/Design Docs & Artifacts

Reports
Risk Analysis, etc)

Process, People & Documentation Evaluation Environment

- Some point tools to assist evaluators but mainly manual work
- Claims in Formal SBVR vocabulary
- Evidence in Formal SBVR vocabulary
- Large scope requires large effort

Process, People, documentation Evidence

Formalized Specifications

Claims, Arguments and Evidence Repository

- Formalized in SBVR vocabulary
- Automated verification of claims against evidence
- Highly automated and sophisticated risk assessments using transitive inter-evidence point relationships

Software System / Architecture Evaluation

- Many integrated & highly automated tools to assist evaluators
- Claims and Evidence in Formal vocabulary
- Combination of tools and ISO/OMG standards
- Standardized SW System Representation In KDM
- Large scope capable (system of systems)
- Iterative extraction and analysis for rules

Software system Technical Evidence

Executable Specifications

Software System Artifacts

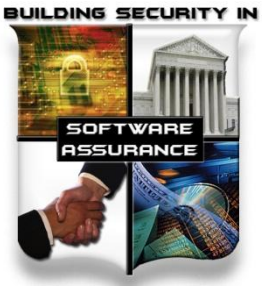
Hardware Environment

Protection Profiles

IA Controls

CWE

IT/Software Supply Chain Management is a National Security & Economic Issue

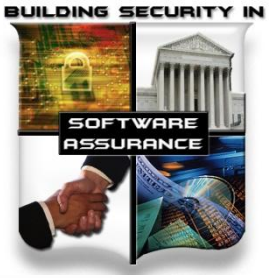


- Adversaries can gain “intimate access” to target systems, especially in a global supply chain that offers limited transparency
- Advances in science and technology will always outpace the ability of government and industry to react with new policies and standards
  - National security policies must conform with international laws and agreements while preserving a nation’s rights and freedoms, and protecting a nation’s self interests and economic goals
  - Forward-looking policies can adapt to the new world of global supply chains
  - International standards must mature to better address supply chain risk management, IT security, systems & software assurance
  - Assurance Rating Schemes for software products and organizations are needed
- IT/software suppliers and buyers can take more deliberate actions to security-enhance their processes and practices to mitigate risks
  - Government & Industry have significant leadership roles in solving this
  - Individuals can influence the way their organizations adopt security practices

Homeland Security

Globalization will not be reversed; this is how we conduct business – To remain relevant, standards and capability benchmarking measures must address “assurance” mechanisms needed to manage IT/Software Supply Chain risks.

Next SwA Working Groups 14-17 Dec 2010 at MITRE, McLean, VA



SOFTWARE ASSURANCE FORUM

"Building Security In"

https://buildsecurityin.us-cert.gov/swa

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

Homeland Security

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Homeland Security

Commerce

National Defense

Next SwA Working Group Sessions 14-17 Dec 2010 at MITRE, McLean, VA