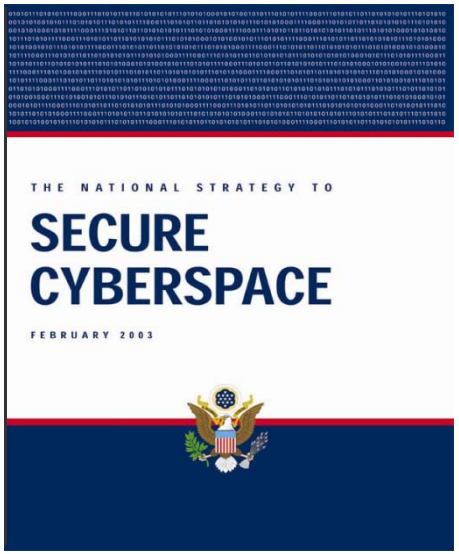
Software Assurance:

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



Application Security:

Mitigating Risks to the Enterprise

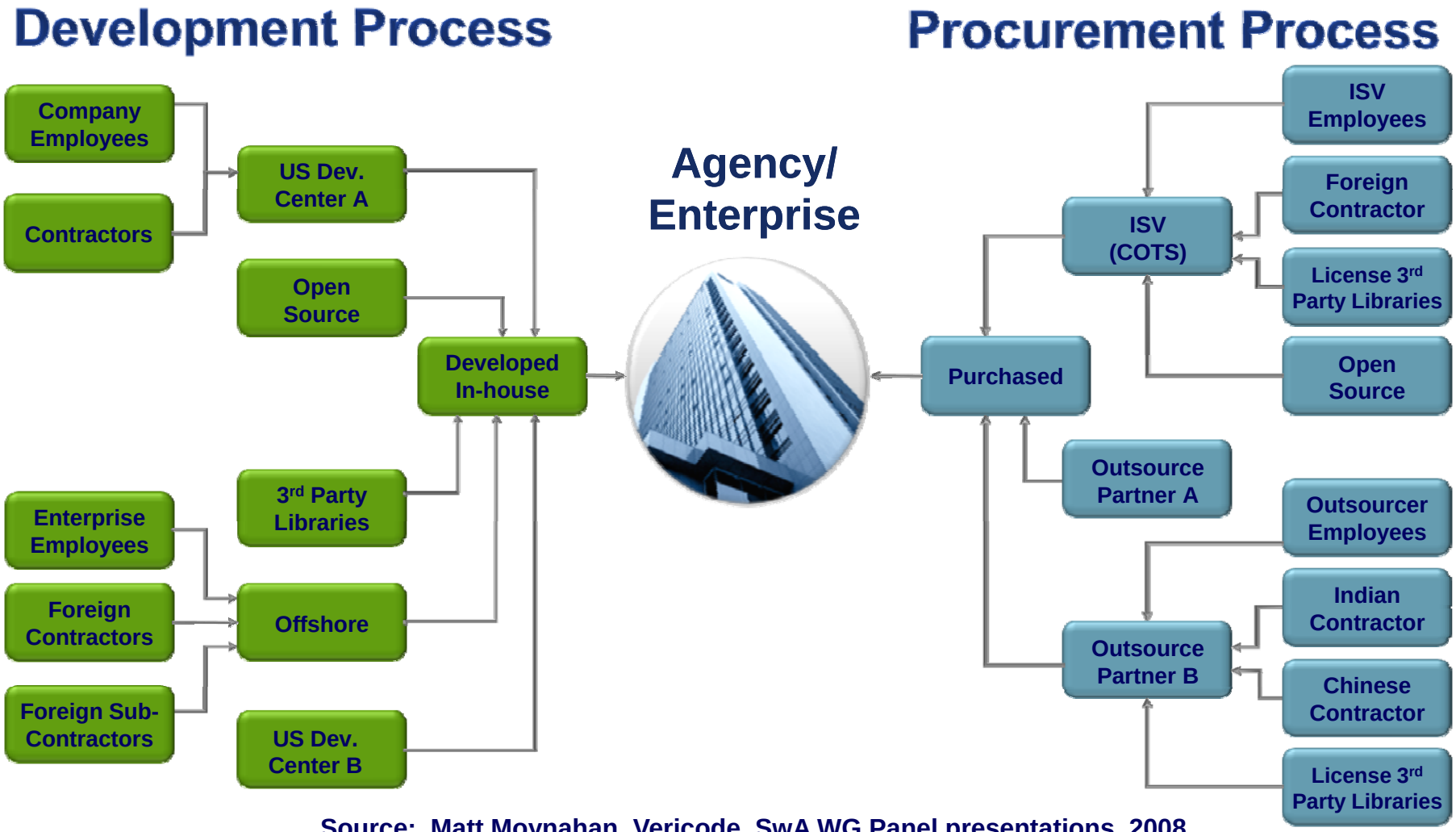
October 2008

Homeland Security

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

Enterprise Processes:
Increasingly Distributed and Complex

New Considerations for Quality & Security



Source: Matt Moynahan, Vericode, SwA WG Panel presentations, 2008

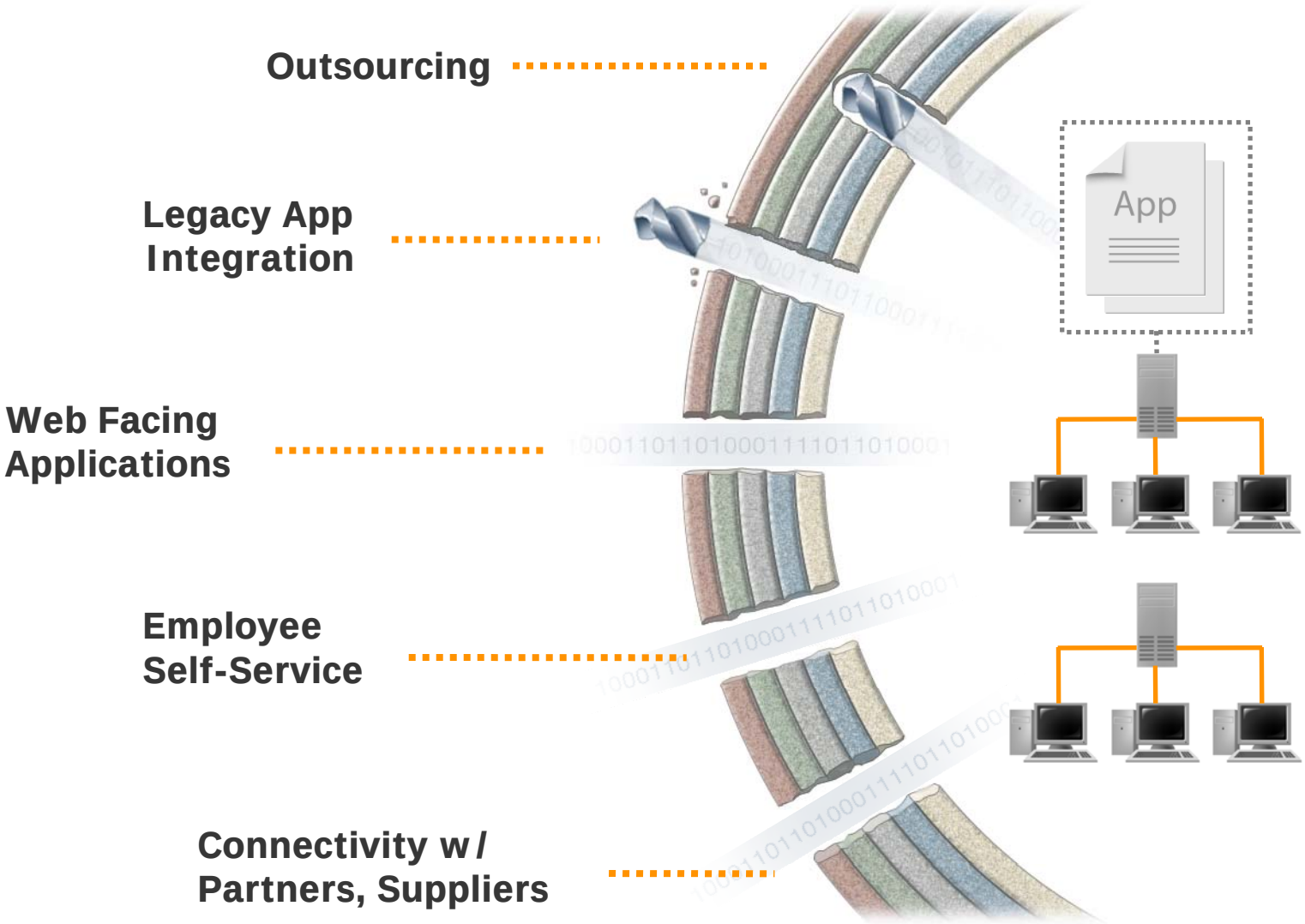
Security-Enhanced Capabilities:
Mitigating Risks to the Enterprise

- 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).
  - 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)

Applications Now Cut Through the Security Perimeter



Homeland Security

"Neutralizing the Threat: A Case Study in Enterprise-wide Application Security Deployments," Bruce C. Jenkins, Fortify Software

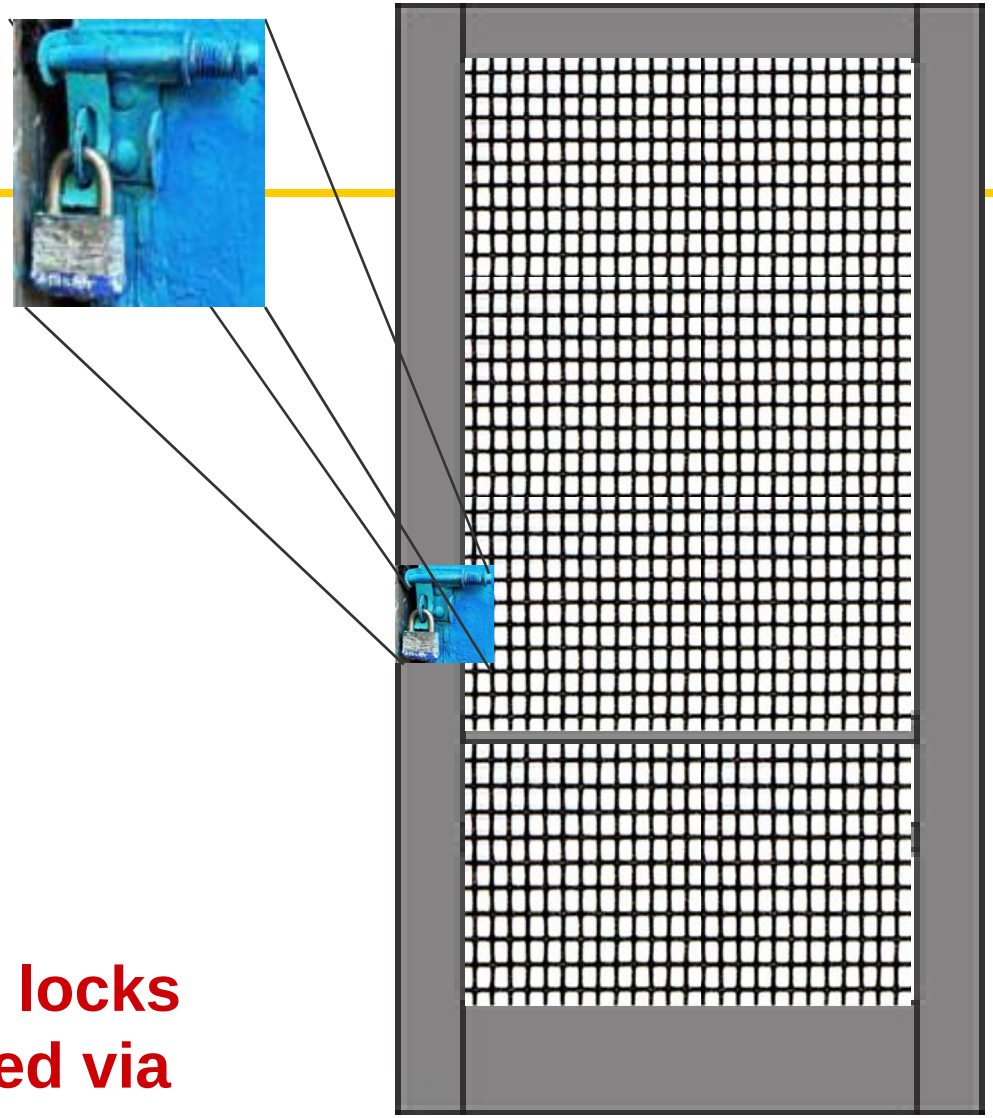
Security is a Requisite Quality Attribute:
Vulnerable Software Enables Exploitation

- 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 and safety must include provisions for built-in security of the enabling software."

Homeland Security

Need for more resilient products



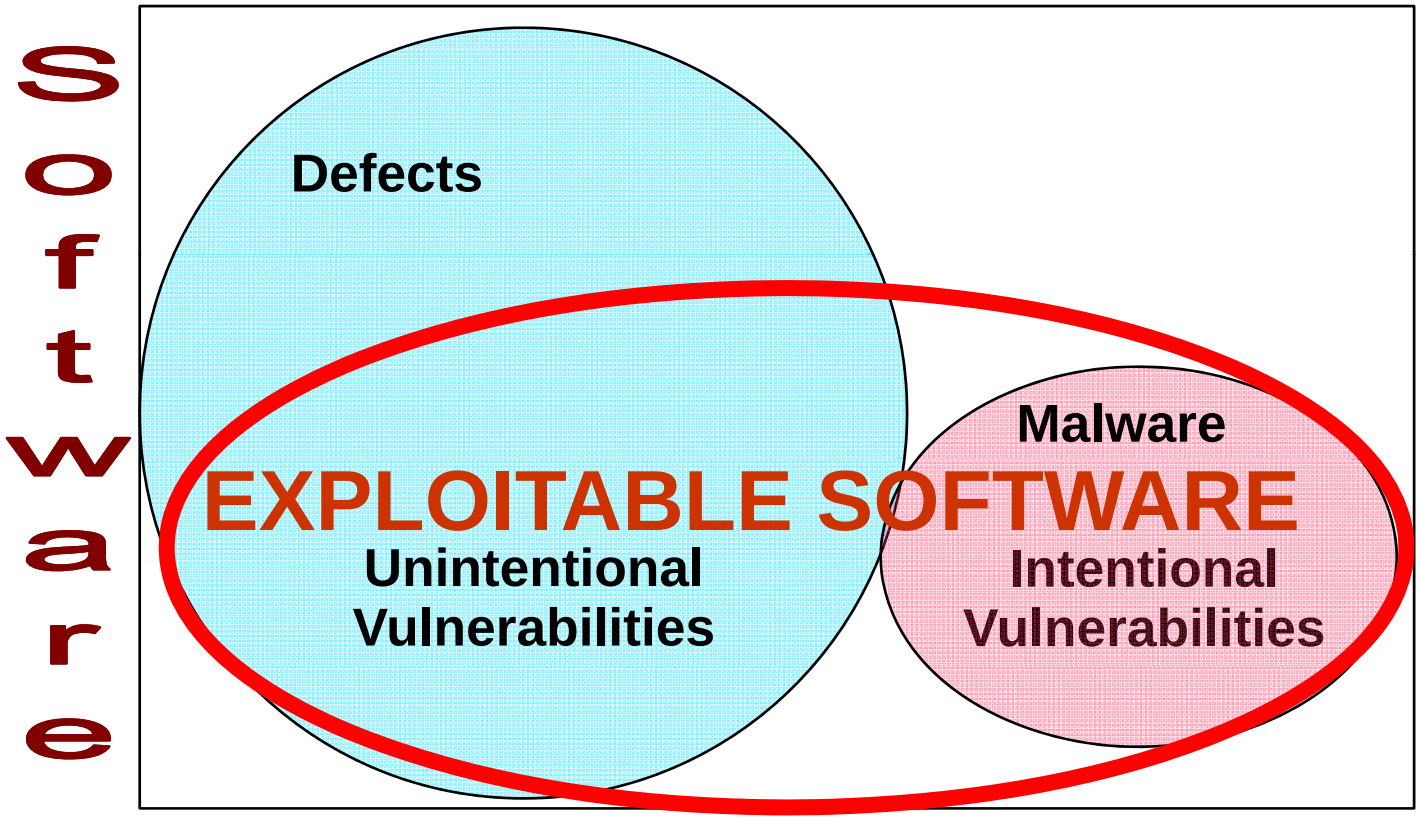
Security Controls are necessary; yet not sufficient, especially when considering the weaknesses in the products to which those controls and protection mechanisms are applied.

There is no need to break locks when access can be gained via exploitable products.

Homeland Security

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

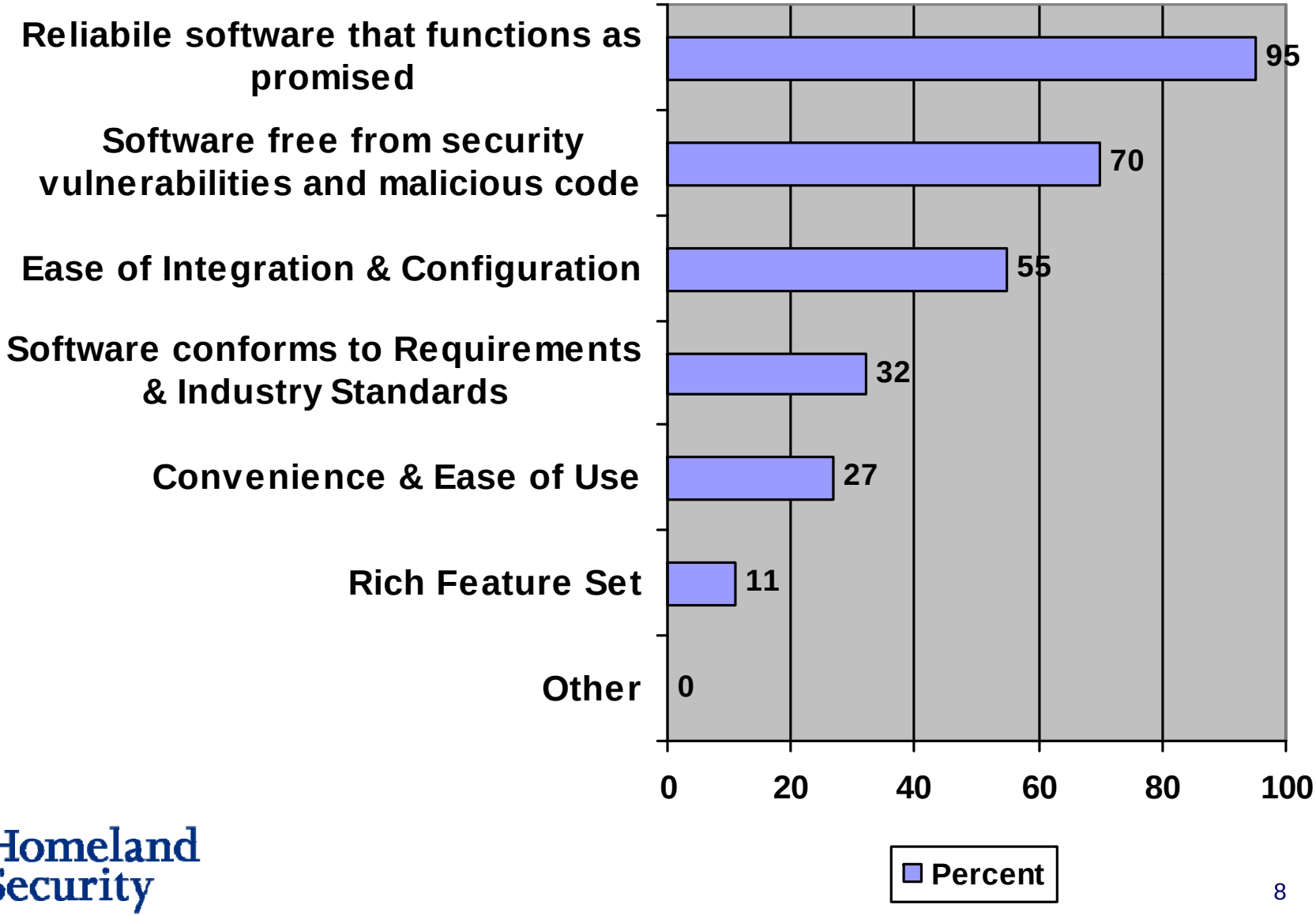
*Intentional vulnerabilities: spyware & malicious logic deliberately imbedded (might not be considered defects)

Homeland Security

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

CIO Executive Council
The Professional Organization for CIOs

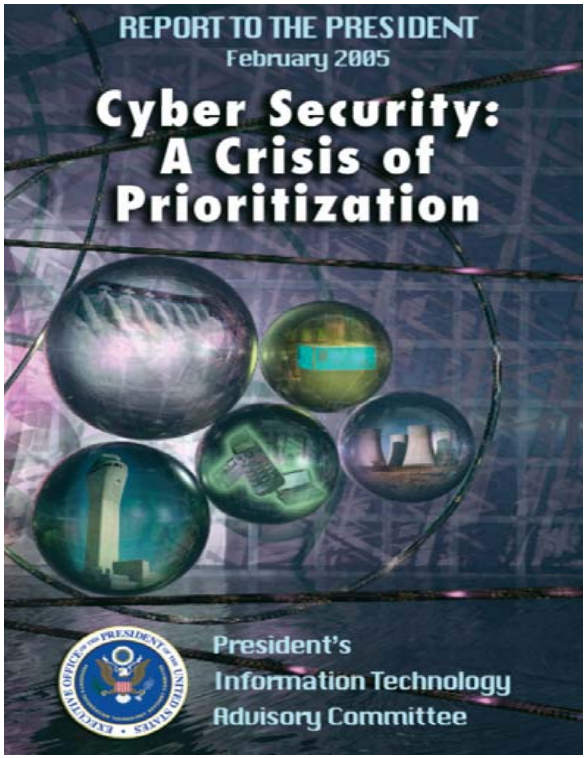
Most Important Attributes



Homeland Security

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]

Homeland Security

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

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

Needs in IT/Software Assurance

- Software & IT lifecycle processes offer opportunities to insert malicious code and to poorly design and build software which enables future exploitation.
- Government and businesses rely on COTS products and commercial developers using foreign and non-vetted domestic suppliers to meet majority of IT requirements.
- Off-shoring magnifies risks and creates new threats to security, business property and processes, and individuals' privacy – requires more comprehensive domestic strategies to mitigate those risks.
- Consumers (Government & industry) lacks information on suppliers' process capabilities (business practices); cannot adequately determine security risks posed by the suppliers' products and services to the acquisition project and to the operations enabled by the software.

Adversaries have capabilities to subvert the IT/software supply chain

Homeland Security

Needs in IT/Software Assurance

- There is a limited number of practitioners that have the requisite knowledge and skills and very few suppliers have adequately incorporated security in their development life cycle.
- Concern about suppliers and practitioners not exercising “minimum level of responsible practice” – no standards in place to benchmark or assess practices.
- Few process improvement and capability appraisal methods and models address security in business practices and process improvement; so security benchmarks are lacking in capability appraisals, and no claims are made about software/system predictable execution.
- Current education & training provides too few practitioners with requisite competencies in secure software engineering – enrollment down in critical IT and software-related degree programs.

Homeland Security

Growing concern about inadequacies of suppliers’ capabilities to build/deliver secure IT/software

What if…

- **Government, in collaboration with industry / academia, raised expectations for product assurance with requisite levels of integrity and security:**
  - Helped advance more comprehensive software assurance diagnostic capabilities to mitigate risks stemming from exploitable vulnerabilities and weaknesses;
  - 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, and products would be securely configured in use.
- **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;
  - Standards and qualified tools would be used to certify software by independent third parties;
  - IT/software workforce had requisite knowledge/skills for developing secure, quality products.

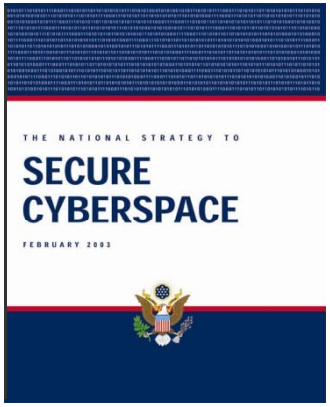
Homeland Security

…Code Transparency could be enabled

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."



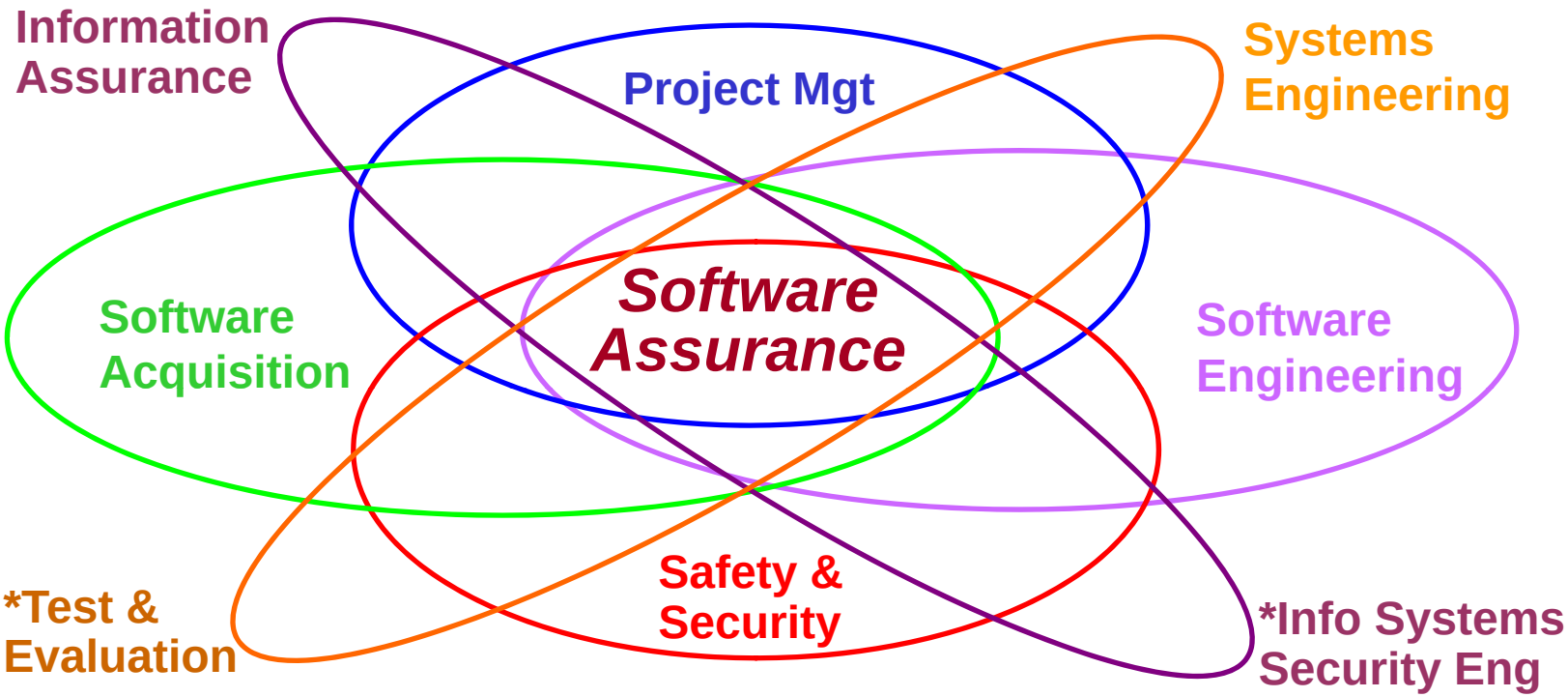
- DHS Program goals promote the security of software across the development, acquisition and implementation life cycle
- DHS Software Assurance (SwA) program is scoped to address:
  - **Trustworthiness** - No exploitable vulnerabilities exist, either maliciously or unintentionally inserted
  - **Dependability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

Also See Wikipedia.org for "Software Assurance"

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".

Homeland Security

Disciplines Contributing to Software Assurance*



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.

DHS Software Assurance Program Structure *

- As part of the DHS risk mitigation effort, the SwA Program seeks to reduce software vulnerabilities, minimize exploitation, and address ways to improve the routine development of trustworthy software products and tools to analyze systems for hidden vulnerabilities.
- The SwA framework encourages the production, evaluation and acquisition of better quality and more secure software; leverages resources to target the following four areas:
  - **People** – education and training for developers 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** – due-diligence questionnaires, contract templates and guidelines for acquisition management and outsourcing

Homeland Security

* July 28, 2006 statement of George Foresman, DHS UnderSecretary for Preparedness, before the U.S. Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Federal Financial Management, Government Information, and International Security

Software Assurance Forum & Working Groups*

… encourage the production, evaluation and acquisition of better quality and more secure software through targeting

People	Processes	Technology	Acquisition
Developers and users education & training	Sound practices, standards, & practical guidelines for secure software development	Security test criteria, diagnostic tools, common enumerations, SwA R&D, and SwA measurement	Software security improvements through due-diligence questions, specs and guidelines for acquisitions/ outsourcing

Products and Contributions

Build Security In - https://buildsecurityin.us-cert.gov and SwA community portal – http://us-cert.gov/SwA

SwA Common Body of Knowledge (CBK) & Glossary
Organization of SwSys Security Principles/Guidelines
SwA Developers' Guide on Security-Enhancing SDLC

Software Security Assurance State of the Art Report

Systems Assurance Guide (via DoD and NDIA)

SwA-related standards – ISO/IEC JTC1 SC7/27/22, IEEE CS, OMG, TOG, & CMM-based Assurance

Practical Measurement Framework for SwA/InfoSec

SwA Metrics & Tool Evaluation (with NIST)
SwA Ecosystem w/ DoD, NSA, NIST, OMG & TOG
NIST Special Pub 500 Series on SwA Tools

Common Weakness Enumeration (CWE) dictionary
Common Attack Pattern Enumeration (CAPEC)
Malware Attribution & Enumeration (with ASC)

SwA in Acquisition: Mitigating Risks to Enterprise Software Project Management for SwA SOAR

Homeland Security

* SwA Forum is part of Cross-Sector Cyber Security Working Group (CSCSWG) established under auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC) that provides legal framework for participation.

Software Assurance Resources

- The DHS National Cyber Security Division serves as a focal point for software assurance, facilitating national public-private efforts to promulgate best practices and methodologies that promote integrity, security, and reliability in software development and acquisition.

- Collaborative efforts of the Software Assurance (SwA) community have produced several publicly available resources:
  - SwA Common Body of Knowledge with Guiding Security Principles (curriculum development guide, updated Oct 2007) at https://buildsecurityin.us-cert.gov/swa/people.html;
  - Securing the Software Lifecycle: Making Application Development Processes - and Software Produced by Them - More Secure, v2.0 (developer's guide, update available Feb 2008);
  - State-of-the-Art Report on Software Security Assurance at http://iac.dtic.mil/iatac/download/security.pdf;
  - Practical Measurement Guidance for SwA and InfoSec, v1.0 (Measurement Guide to support information needs; draft update available Mar 2008);
  - Software Assurance in Acquisition: Reducing Risks to the Enterprise, v1.0 (procurement guide - https://buildsecurityin.us-cert.gov/daisy/bsi/resources/dhs/908.html);
  - State-of-the-Art Report on Software Project Management for Software Assurance https://buildsecurityin.us-cert.gov/daisy/bsi/resources/dhs/906.html
  - Common Attack Pattern Enumeration and Classification (CAPEC - http://capec.mitre.org), and
  - Common Weakness Enumeration (CWE - http://cwe.mitre.org) with links to the National Vulnerability Database - http://nvd.nist.gov/nvd.cfm.

- For more information, see Build Security In web site https://buildsecurityin.us-cert.gov/ -- expanding to become the Software Assurance (SwA) Community of Practice portal http://www.us-cert.gov/swa to provide coverage of topics relevant to the broader stakeholder community.

Homeland Security

DHS Software Assurance (SwA) Outreach

- Co-sponsor bi-monthly SwA WG sessions and semi-annual Software Assurance Forum for government, academia, and industry to facilitate ongoing collaboration -- next Oct 14-16, 2008 at NIST in Gaithersburg MD
- Co-sponsor SwA issues of CROSSTALK (since Oct 05); provide SwA articles in other journals to "spread the word" to relevant stakeholders
  - March 2007 issue on "Software Security"
  - May 2007 issue on "Software Acquisition"
  - Sep 2007 issue on "Service Oriented Architecture"
  - June 2008 issue on "Software Quality"
  - Sep 2008 issue on "Application Security
- Provide free SwA resources via "BuildSecurityIn" portal to promote relevant methodologies (since Oct 05)
- Host http://www.us-cert.gov/SwA/ for Software Assurance Community of Practice (since Dec 07)
- Provide DHS Speakers Bureau speakers
- Support efforts of consortiums and professional societies in promoting SwA

Homeland Security

INPUT

TargetVIEW

Process Agnostic Lifecycle

Launched 3 Oct 2005

Architecture & Design
- Architectural risk analysis
- Threat modeling
- Principles
- Guidelines
- Historical risks
- Modeling tools
- Resources

Code
- Code analysis
- Assembly, integration & evolution
- Coding practices
- Coding rules
- Code analysis
- Resources

Test
- Security testing
- White box testing
- Attack patterns
- Historical risks
- Resources

Requirements
- Requirements engineering
- Attack patterns
- Resources

Touch Points & Artifacts

System
- Penetration testing
- Incident management
- Deployment & operations
- Black box testing
- Resources

Fundamentals
- Risk management
- Project management
- Training & awareness
- Measurement
- SDLC process
- Business relevance
- Resources

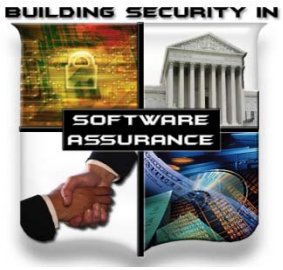
Key
- Best (sound) practices
- Foundational knowledge
- Tools
- Resources

https://buildsecurityin.us-cert.gov

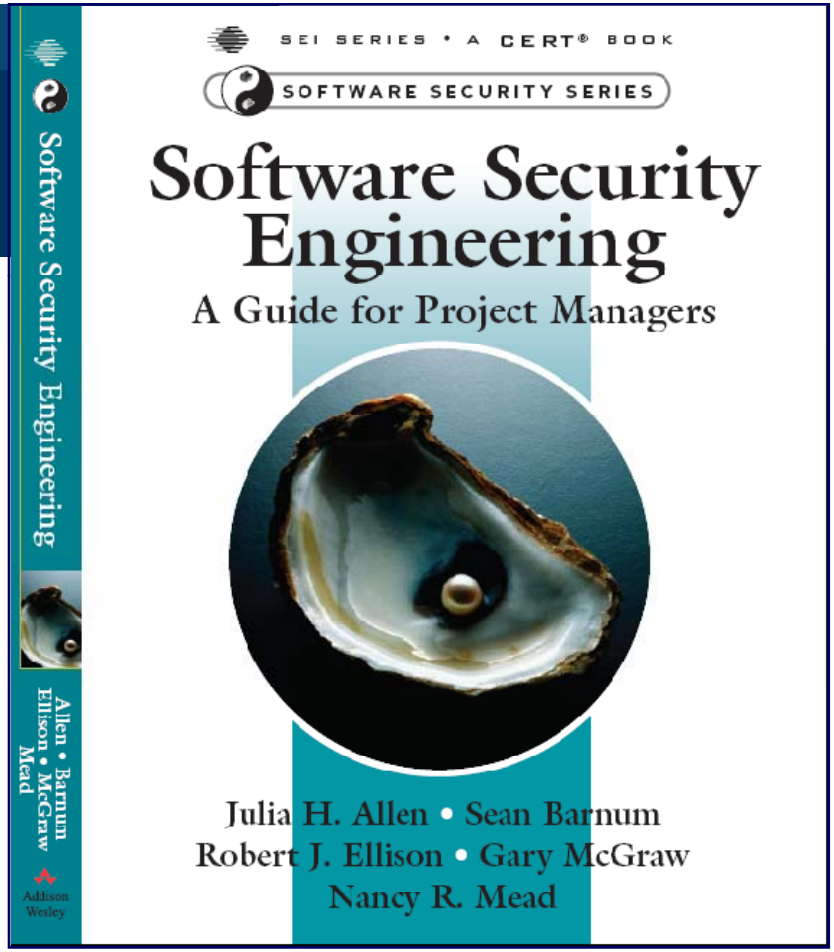
Homeland Security

BUILDING SECURITY IN
SOFTWARE ASSURANCE

Software Security Engineering: A Guide for Project Managers



- Organized for Project Managers
  - Derives material from DHS SwA "Build Security In" web site
    - https://buildsecurityin.us-cert.gov
  - Provides a process focus for projects delivering software-intensive products and systems
- Published in May 2008



Homeland Security

Software Assurance

Community Resources and Information Clearinghouse

Sponsored by DHS National Cyber Security Division

Working Groups

Workforce Education & Training

Processes & Practices

Technology, Tools & Product Eval.

Acquisition & Outsourcing

Measurement

Business Case

Malware Attribution

Join a Working Group

US-CERT Software Assurance

Build Security In

Software assurance (SwA) is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner (from CNSS 4009 IA Glossary - see Wikipedia for definitions and descriptions).

As part of the DHS risk mitigation effort, the Software Assurance Program seeks to reduce software vulnerabilities, minimize exploitation, and address ways to improve the routine development of trustworthy software products with predictable execution, and to improve diagnostic capabilities to analyze systems for hidden vulnerabilities.

The **Software Assurance Forum** and several **working groups** composed of volunteers from government, industry, and academia are helping the Software Assurance Program achieve its objectives. The next Software Assurance Forum is May 6-8 in McLean, Virginia. The current active working groups are

- Workforce Education & Training
- Processes & Practices
- Technology, Tools & Product Evaluation
- Acquisition & Outsourcing
- Measurement
- Business Case
- Malware Attribution

WHY IS SOFTWARE ASSURANCE CRITICAL?

The nation's critical infrastructure (energy, transportation, telecommunications, etc.), businesses, and services are extensively and increasingly controlled and enabled by software. Vulnerabilities in that software put those resources at risk. The risk is compounded by software size and complexity, the use of software produced by unvetted suppliers, and the interdependence of software systems. Software assurance deals with the root of the problem by improving software security.

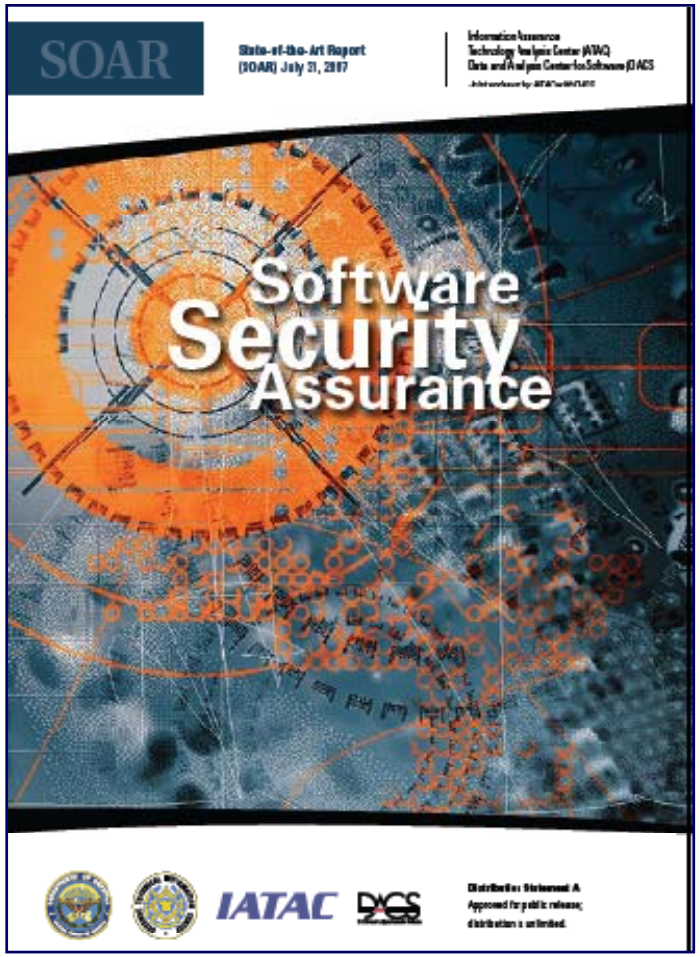
HOW IS SOFTWARE ASSURANCE ADVANCING?

The Software Assurance Forum has provided a collaborative venue for stakeholders to share and advance techniques and technologies relevant to software security. Software Security Assurance: A State-of-the-Art Report (SOAR) represents an output of collaborative efforts of organizations and individuals in the SwA Forum and working groups. The SOAR provides an overview of the current state of the environment in which software must operate and surveys current and emerging activities and organizations involved in promoting various aspects of software security assurance

Software Security Assurance:

A State of the Art Report, 31 July 2007

- FREE publicly available resource provides a comprehensive look at efforts to improve the state of Software Security Assurance:
  - describes the threats and common vulnerabilities to which software is subject;
  - presents the many ways in which the S/W Security Assurance problem is being framed and understood across government, industry, and academia;
  - describes numerous methodologies, best practices, technologies, and tools currently being used to specify, design, and implement software that will be less vulnerable to attack, and to verify its attack-resistance, attack-tolerance, and attack-resilience;
  - offers a large number of available print and online resources from which readers can learn more about the principles and practices that constitute Software Security Assurance;
  - provides observations about potentials for success, remaining shortcomings, and emerging trends across the S/W Security Assurance landscape.



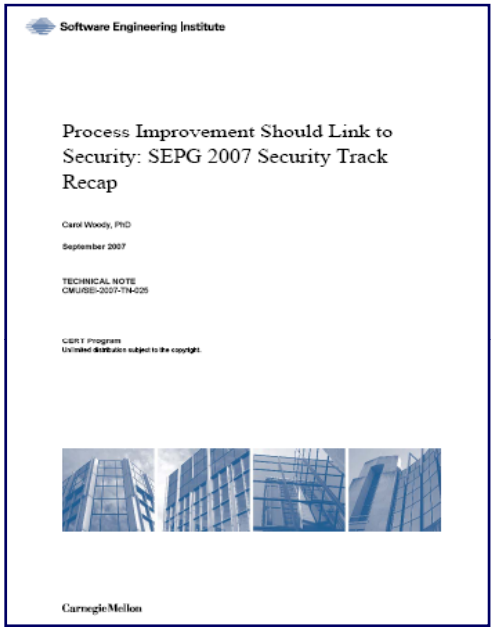
- Free via http://iac.dtic.mil/iatac/download/security.pdf
  - IATAC, an Information Analysis Center in Defense Technical Information Center
  - *The SOAR reflects output of efforts in the DoD-DHS Software Assurance Forum and Working Groups that provide collaborative venues for stakeholders to share and advance techniques and technologies relevant to software security.*

Deloittes 2007 ***Global Security Survey: The Shifting Security Paradigm*** provides relevant insights about software security in financial services

- Eight Key Findings of Survey, aligned with Gartner and Software Assurance findings
- #3 Application Security: Generic Countermeasures are No Longer Adequate – notes ***decisions in software development lifecycle significantly impact financial operations***
  - It is becoming very clear that decisions made during the software development lifecycle—from user interface design to facilities for patch management—can significantly impact the likelihood of security incidents and the success of a response to them.
  - A recent Gartner summit revealed that application security is the number one issue for CIOs.
    - Yet when asked whether their organizations have incorporated application security as part of their software development lifecycle, responses were extremely low across the board
    - To remain competitive, organizations must mitigate software security risks when they acquire, outsource, implement, or host software applications.
  - Information Security team must continually raise the bar for secure software development by:
    - 1) examining software developed internally;
    - 2) demanding trustworthy software from vendors and business partners, and
    - 3) ensuring that applications have the adequate controls for audit trails.
  - There must be no ambiguity around the premise that **applications are the primary gateway to sensitive data and must be secured from the ground up**.
- Under Quality of Operations, on page 36, the report notes: ***As organizations acquire, outsource, implement and host applications, they must recognize and mitigate software security risks.***
  - Application security means ensuring that there is secure code, integrated at the development stage, to prevent potential vulnerabilities and that steps such as vulnerability testing, application scanning and penetration testing are part of an organization's software development lifecycle.
  - This year, 87% of respondents feel poor software development quality is a top threat envisioned over the coming 12 months.

Process Improvement Should Link to Security:
SEPG 2007 Security Track Recap

http://www.sei.cmu.edu/publications/documents/07.reports/07tn025.html


Software Engineering Institute

Process Improvement Should Link to Security: SEPG 2007 Security Track Recap

Carol Woody, PhD

September 2007

TECHNICAL NOTE
CMU/SEI-2007-TN-025

CERT Program
Unlimited distribution subject to the copyright.

Carnegie Mellon

1 Process Improvement Should Link to Security

- Panel Questions, Presentations and Resources
- Getting Credit for Effective Security Processes
- Processes for Determining Security Requirements
- Measuring Security Processes & Improvement Efforts
- Development Processes Contributing to Operational Resiliency
- Leveraging Process Improvement for Security in the SDLC
- Audience Feedback To Panelists

2 Security Track Presenters Connect Security to Process

2.1 Security Track Speakers Covered A Range of Security Issues
2.2 Software Security— Setting the Stage
2.3 Insider Threats in the SDLC
2.4 Engineering Safety- and Security-Related Requirements for Software-Intensive Systems
2.5 Focus on Resiliency: A Process Improvement Approach to Security
2.6 Getting Started with Measuring Your Security

3 Strengthening Ties between Process and Security

3.1 Security Birds of a Feather (BOF) at SEPG07
3.2 NDIA Systems Assurance Guidebook
3.3 DHS Software Assurance Program
3.4 ISSEA Systems Security Engineering CMM
3.5 ISO/IEC 15026 “Systems and Software Assurance”

Homeland Security

Making Process Improvements for Security

Lessons learned indicate a need to understand how to leverage best practices to effectively implement application security tools and methods.

- Understand existing development environment
- Define relevant coding standards and policies
- Define roles and responsibilities
- Provide Awareness and Training programs
- Develop security risk management process framework
- Expose security needs and requirements
- Integrate threat modeling during design phase
- Integrate automated security code scanning
- Define goals and metrics for application security

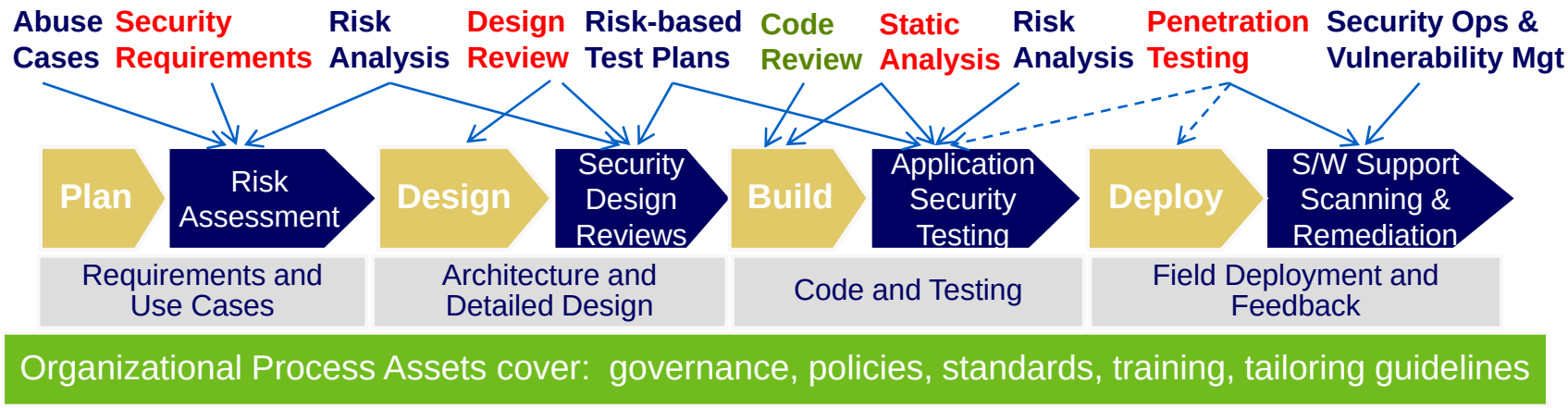
Homeland Security

* Adopted in part from DHS SwA Working Group sessions and "What to Test from a Security Perspective: An Introduction to Security Testing for the QA Professional" (Cigital) and "Neutralizing the Threat: A Case Study in Enterprise-wide Application Security Deployments" (Fortify Software & Accenture Security Technology Consulting)

Security-Enhanced Process Improvements

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

"Build Security In" throughout the lifecycle



- Modifying the SDLC to incorporate security processes and tools should be done in phases
- Allow for time to change culture and processes
- Avoid drastic changes to existing development environment
- Balance benefits and determine best integration points

Homeland Security

* Adopted in part from "What to Test from a Security Perspective: An Introduction to Security Testing for the QA Professional" (Cigital) and "Neutralizing the Threat: A Case Study in Enterprise-wide Application Security Deployments" (Fortify Software & Accenture Security Technology Consulting)

Enhance "Assurance" Considerations:
Leveraging CMM-based Process Improvement

Determine how "assurance" has been factored into suppliers' process capabilities

- **An infrastructure for safety & security is established and maintained.**
  1. Ensures Safety and Security Competency within the Workforce;
  2. Establishes a Qualified Work Environment (including the use of qualified tools);
  3. Ensures Integrity of Safety and Security Information;
  4. Monitors Operations and Report Incidents (relative to the deployed environment);
  5. Ensures Business Continuity.
- **Safety & security risks are identified and managed.**
  6. Identifies Safety and Security Risks;
  7. Analyzes and Prioritizes Risks relative to Safety and Security;
  8. Determines, Implements, and Monitors the associated Risk Mitigation Plan.
- **Safety & security requirements are satisfied.**
  9. Determines Regulatory Requirements, Laws, and Standards;
  10. Develops and Deploys Safe and Secure Products and Services;
  11. Objectively Evaluates Products (using safety and security criteria);
  12. Establish Safety and Security Assurance Arguments (with supporting evidence).
- **Activities/products are managed to achieve safety & security requirements/objectives.**
  13. Establishes Independent Safety and Security Reporting;
  14. Establishes a Safety and Security Plan;
  15. Selects and Manages Suppliers, Products, and Services using safety and security criteria;
  16. Monitors and Controls Activities and Products relative to safety and security requirements.

Many suppliers use CMMs to guide process improvement & assess capabilities; yet many CMMs do not explicitly address safety and security.

Source for "Assurance" enhanced processes: *U.S. DoD and FAA joint project on Safety and Security Extensions for Integrated Capability Maturity Models, September 2004,* at http://www.faa.gov/about/office_org/headquarters_offices/aio/documents/media/SafetyandSecurityExt-FINAL-web.pdf

CMMI "Assurance" Focus Area

- Integrates assurance considerations in the development lifecycle
- Creates a draft set of assurance goals and practices
- Harmonizes System Security Engineering Capability Maturity Model (SSE-CMM) & Motorola Secure Software Development Model (MSSDM) within CMMI architecture
- Consistent with existing CMMI-DEV v1.2
- Supports joint capability appraisals to provide a measurement benchmark
- Relatively stable
- Applicable in diverse contexts (defense, health, finance, etc)
- Can be used for process implementation, evaluation, and improvement of assurance process capability
- Requires minimal level of effort to implement within current CMMI implementations
- Assurance activities are "built in" to other processes as a part of the SDLC
- Can be completed within Focus Topic Guidelines

Homeland Security

CMMI Process Reference Model (PRM) Goals and Practices for "Assurance"

All PRM Specific Practices map to a CMMI-Dev v1.2 Specific Practice	Goals	Specific Practices
PA: Assurance Process Management	5	20
PA: Assurance Project Management	1	5
PA: Assurance Engineering	4	17
PA: Assurance Support Activities	3	16
Total	**13**	**58**

Homeland Security

CMMI Assurance Thread

Process Reference Model (PRM) for Assurance			CMMI Thread Location	
Process Area: Assurance Process Management			**Target PA(s)**	**PA and SP**
Goal: SG1.1 - Establish the assurance process environment to achieve key business goals.				
	Specific Practice 1.1.1 Identify the business goals for assurance.		OPF Organizational Process Focus	OPF SP 1.1 Establish Organizational Process Needs
		Sub Practice 1.1.1.1 Identify the assurance stakeholders including their expectations and rights.		
		Sub Practice 1.1.1.2 Quantify business value of assurance.		
		Sub Practice 1.1.1.3Determine quality related assurance objectives and select model and standards(CMMI C&A, ISO-27000,ISO-9000, Common Criteria etc.) which best aligns with organizational objectives.		
		Sub Practice 1.1.1.4 Determine the business continuity needs for process assets and support infrastructure including Process Asset Library and measurement infrastructure.		
		Sub Practice 1.1.1.5 Prioritize the business goals for assurance.		

Color Legend

Blue: PRM Process Area
Yellow: PRM Goals
Green: PRM Practices that support a goal
Purple: PRM Informative material to assist with implementing practices
Pink: CMMI Process Areas
Orange: CMMI Specific Practices that support a goal

Homeland Security

Measurement Practices

Process Reference Model for Assurance				CMMI Thread Location	
PRM Process ea	**PRM Goals**	**PRM Practices that support a goal**	**PRM Informative material to assist with implementing practices**	**CMMI Process Areas**	**CMMI Specific Practices that support a goal**
Process Area: Assurance Project Management				**Target PA(s)**	**PA and SP**
Goal: SG2.2 -Establish and maintain an assurance support activities for the project.					
	Specific Practice 2.2.4 Measure effectiveness of project assurance goals.			MA Measurement and Analysis	SP 1.1 Establish measurement objective SP 1.2 Specify measures.
		Sub Practice 2.2.4.1 Define project assurance goals and measures.			
		Sub Practice 2.2.4.2 Collect project assurance data to support organizational assurance measures.			MA SP 2.1 - Collect Measurement Data
		Sub Practice 2.2.4.3 Store assurance measures with project artifacts.			MA SP 2.3 - Store data and results.
		Sub Practice 2.2.4.4 Analyze collected project assurance measures and develop assurance case.			MA SP 2.2 - Analyze measurement data
		Sub Practice 2.2.4.5 Report assurance measures to the appropriate stakeholders			MA 2.4 Communicate results.
		Sub Practice 2.2.4.6 Practice continuous improvement of the measures due to issues identified in the measures.			MA SP 1.2 Specify Measures MA SP 2.2 Analyze Measurement Data

Color Legend

Blue: PRM Process Area
Yellow: PRM Goals
Green: PRM Practices that support a goal
Purple: PRM Informative material to assist with implementing practices
Pink: CMMI Process Areas
Orange: CMMI Specific Practices that support a goal

Homeland Security

Enhancing the Development Life Cycle to Produce Secure Software

- Document produced by the DHS NCSD SwA Process Working Group
- Aimed at software developers, architects, integrators, testers, SwA SMEs
- Available Oct 2008 through the DoD Data and Analysis Center for Software in pdf and Wiki form
- Broad base of contributors from industry, government, vendors, and academia
- Provides *objective* information on a range of processes, methodologies, practices, and techniques for security-enhancing the SDLC
- Extensive lists of references to further information on all key topics, including OWASP

Homeland Security

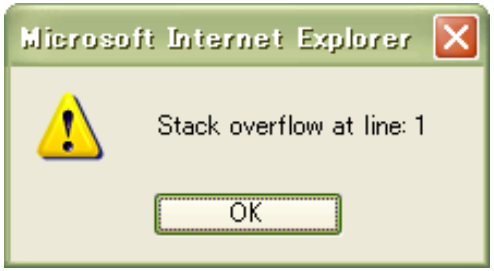
Enhancing the Development Life Cycle
50,000 Foot View

Section	Content	Who will benefit most from reading?
1	Introduction: Document purpose, intended audience, structure, and content description	All
2	Background: Understanding the problem	All
3	Integrating security into the SDLC	All
4	Requirements for secure software	Requirements analyst, Tester, PM
5	Secure design principles and practices	Architect, Designer, Integrator
6	Secure component-based software engineering	Architect, Integrator
7	Secure coding principles and practices	Programmer
8	Risk-based software security testing	Tester
9	Secure distribution, deployment, and sustainment	Integrator, PM, Maintainer
App. A	Abbreviations, acronyms, and definitions	All
App. B	Resources and Bibliography	All

Homeland Security

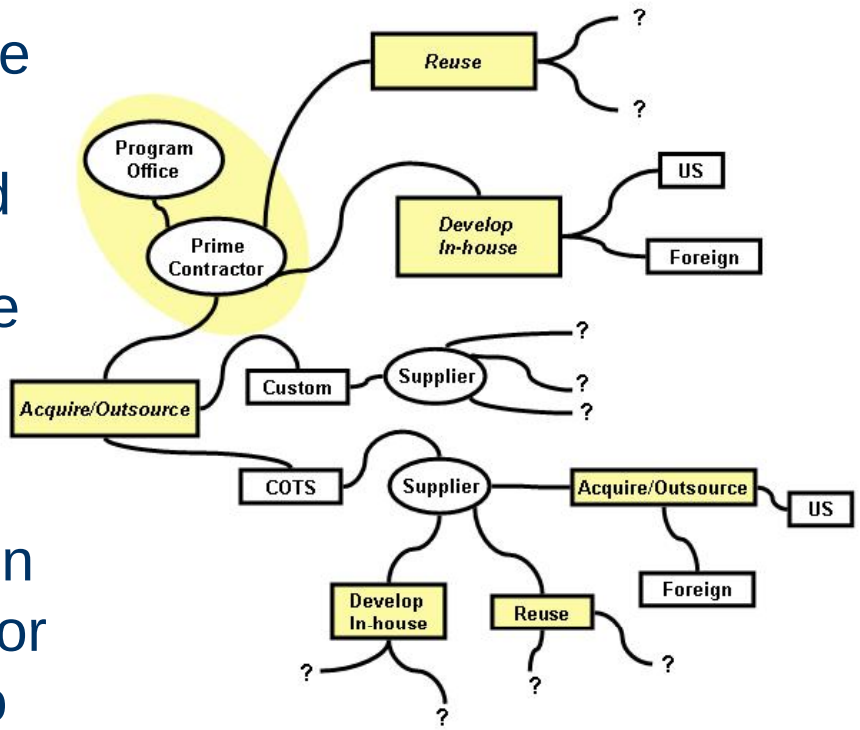
While more guidance is available, growing concern about inadequacies of suppliers' capabilities to deliver secure software

- Unknown development practices
  - How was the software built? What methodologies, practices, tools were used?
- Lack of visibility (the "black box" problem) (*OTS, legacy)
  - Questionable validity of security assumptions able to be made based solely on external observation of executing software
- Unknown review and testing regime
  - Only safe assumption: security was not considered during reviews, tests
- Security in sustainment
  - How committed is the supplier/development team long term to maintenance and patching?
  - Does the supplier/development team support bug and vulnerability reporting and tracking, with timely response?



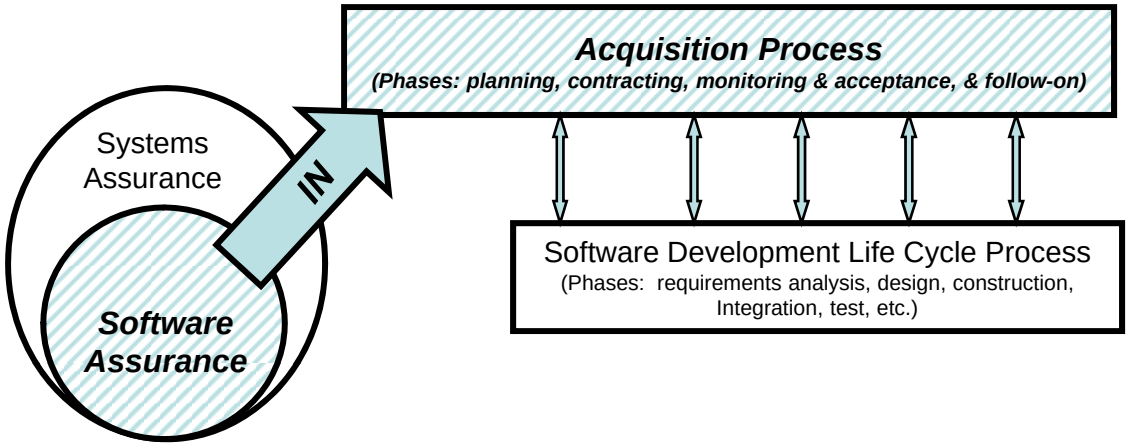
Software Assurance must now be considered when acquiring software by contract

- Stakeholders now need justifiable confidence that the software that enables their core business operations can be trusted to function as expected
- Responsibility for SwA must be shared by the Acquirer in the software supply chain
- Therefore, acquirers involved in purchasing software products or services has a responsibility to factor in SwA to minimize software risks



Homeland Security

SwA Working Group produced document to help "build security in" and incorporate SwA considerations throughout the acquisition process



- Written from an acquisition process perspective versus the software development lifecycle process perspective
- For anyone, both government and private sector, involved in acquiring software products or services by contract, including work that is outsourced or sub-contracted
- NOT an exhaustive coverage of SwA considerations when acquiring software

Homeland Security

Software Assurance in Acquisition: Mitigating Risks to the Enterprise

Version 1 published Oct 2008 through National Defense University (NDU) Press via Information Resource Management College (IRMC)

Executive Summary

1. Introduction

1.1 Background

1.2 Purpose and Scope

1.3 Audience—The Acquirer

1.4 Document Structure

2. Planning Phase

2.1 Needs Determination, Initial Risk Assessment, and Solution Alternatives

2.2 SwA Requirements

2.3 Acquisition Strategy and/or Plan

2.4 Evaluation Plan and Criteria

2.5 SwA Due Diligence Questionnaires

3. Contracting Phase

3.1 Request for Proposals

3.1.1 Work Statement

3.1.2 Terms and Conditions

3.1.3 Instructions to Suppliers

3.1.4 Certifications

3.1.5 Prequalification

3.2 Proposal Evaluation

3.3 Contract Negotiation and Contract Award

4. Implementation and Acceptance Phase

4.1 Contract Work Schedule

4.2 Change Control

4.3 Reviewing and Accepting Software Deliverables

5. Follow-on Phase

5.1 Sustainment (or Post Release Support)

5.1.1 Risk Management

5.1.2 Assurance Case Management—Transition to Ops

5.1.3 Change Management Considerations

5.2 Disposal or Decommissioning

Homeland Security

Software Assurance (SwA) Acquisition Handbook

Appendix A— Acronyms

Appendix B— Glossary

Appendix C— An Imperative for SwA in Acquisition

Appendix D— Software Due Diligence Questionnaires (Examples)

- Table D-1. COTS Software Questionnaire
- Table D-2. Open-Source Software Questionnaire
- Table D-3. Custom Software Questionnaire
- Table D-4. GOTS Software Questionnaire
- Table D-5. Software Services

Appendix E— Other Examples of Due Diligence Questionnaires

Appendix F— Sample Language for the RFP and/or Contract

- F.1 Security Controls and Standards
- F.2 Securely Configuring Proprietary Commercial Software
- F.3 Acceptance Criteria
- F.4 Certifications
- F.5 Sample Instructions to Offerors Sections
- F.6 Sample Work Statement
- F.7 Open Web Application Security Project
- F.8 Certification of Originality
- F.9 Other Source of SwA Requirements

Appendix G— References

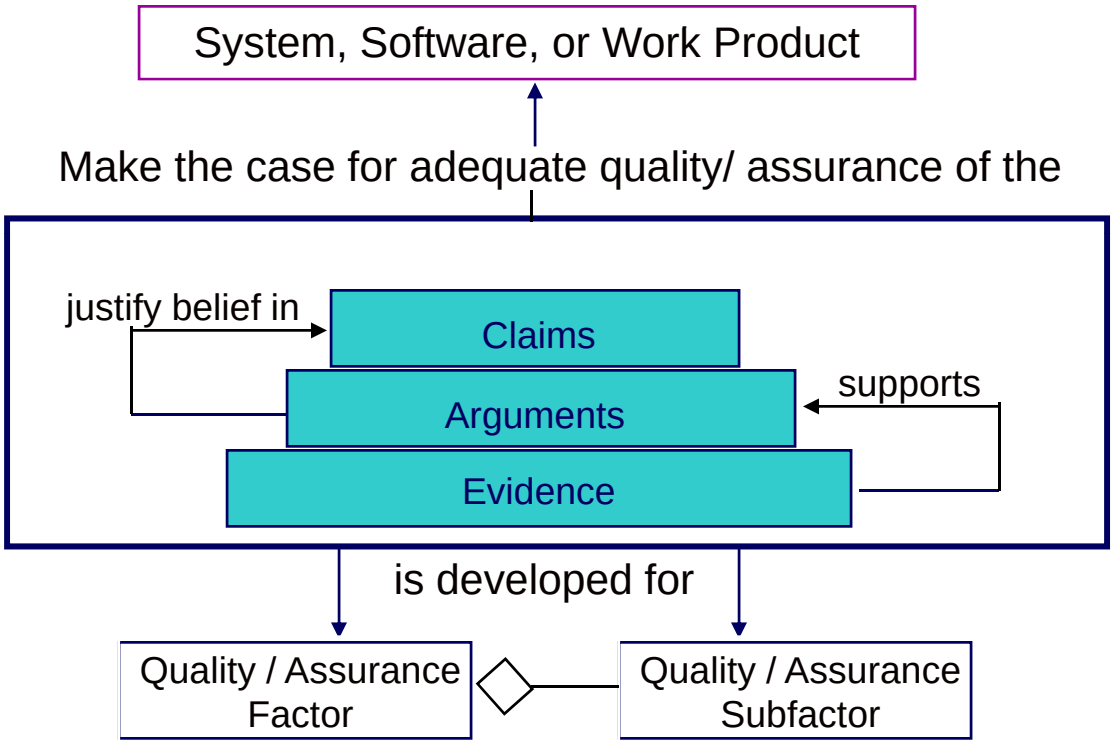
Getting Started: Use Appendices Now

Homeland Security

Suppliers should be able to describe an Assurance Case for their software and explain how claims can be validated

What constitutes sufficient Evidence to support Arguments that justify Claims?

How might "scaling" be structured to enable and encourage more suppliers and acquirers to make use of assurance cases?



Adopted from US TAG ISO/IEC 15026 proposal May 2007 and CMU SEI QUASAR tutorial by Donald Firesmith, March 2007

Due Diligence Questionnaires address different software types and SwA concerns and can be used to evaluate software/suppliers

Questions are organized into categories of SwA concerns

Assurance Claims and Evidence	
52	Does your company develop security measurement objectives for phases of the SDLC? Has your company identified specific statistical and/or qualitative analytical techniques for measuring attainment of security measures?
53	Has the software been measured/assessed for its resistance to identified relevant attack patterns? Are Common Vulnerabilities & Exposures (CVE®) or Common Weakness Enumeration (CWEs) used? How have the findings been mitigated?
54	Are static or dynamic software security analysis tools used to identify the weaknesses that can lead to exploitable vulnerabilities in the software? If yes, which tools are used? What classes of weaknesses are covered? When in the SDLC are these scans performed? Are SwA experts involved in the analysis of the scan results?
55	Does the software contain third-party developed components? If yes, are those components scanned by a static code analysis tool?
56	Has the software undergone any penetration testing? When? By whom? Are the test reports available under a nondisclosure agreement? How have the findings been mitigated?
57	Are there current publicly-known vulnerabilities in the software (e.g., an unrepaired CWE entry)?
58	How is the assurance of software produced by third-party developers assessed?

Homeland Security

SwA Measurement Activities

- SwA Processes and Practices WG – promotes integration of assurance into system and software development standards and methodologies and development of processes and tools for that purpose
  - Processes and Practices participates in industry WG to develop CMMI Assurance Focus Area

    https://buildsecurityin.us-cert.gov/swa/downloads/PRM_for_Assurance_to_CMMI.pdf
- SwA Measurement WG – works to address assessing assurance provided by software, using quantitative and qualitative methodologies and techniques
  - Developing Practical Framework for Software Assurance and Information Security Measurement

    https://buildsecurityin.us-cert.gov/swa/downloads/SwA_Measurement.pdf
  - Populating a web site of software assurance measurement resources https://buildsecurityin.us-cert.gov/swa/measact.html

Homeland Security

The Business Case for Software Assurance

- Products with built in security:
  - Are more resilient and cost less to sustain
  - Require less rework prior to being put into use
- Resources are available to assist organizations in integrating security practices in their software lifecycle.
- Lessons learned indicate a need to understand how to leverage best practices to effectively implement application security tools and methods.
  - Application Security requires Processes and Practices that span development, acquisition, and use
  - Processes and Practices must be supplemented with qualified security tools
  - Measurement (including benchmarking of process capabilities) supports decision-making
- Information is publicly available for “Making the Business Case for Software Assurance”

Homeland Security

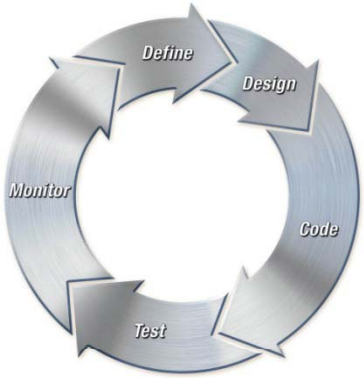
Security-Enhanced Best Practices

- Existing, successful development and acquisition processes should not be altered significantly to accommodate tools—application security tools should be adapted whenever possible to your existing processes
- When you do make process changes, do so incrementally and only for the sake of improvements that provide a reduction in risk and/or measurable return on investment

❑ Security Risk-based Requirements Considerations:

-- What (could go wrong)
-- Who (would cause it)
-- How (could it be done)

Everyone's Responsibility



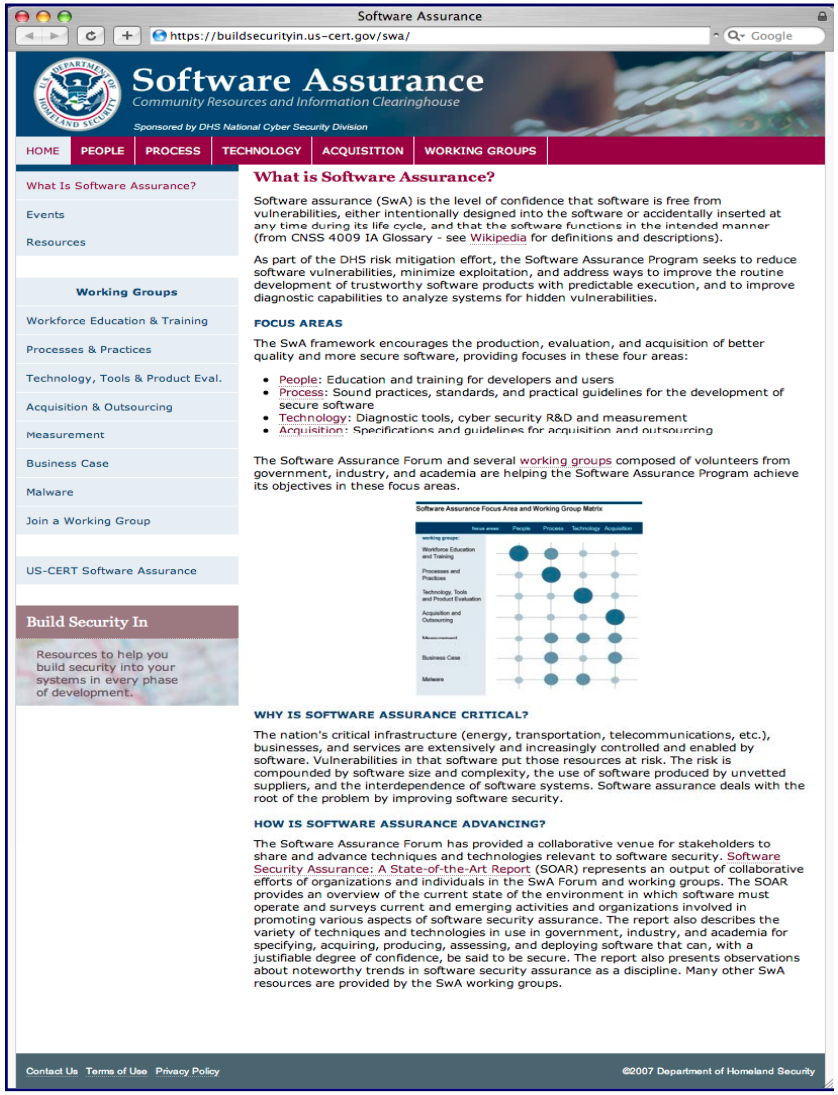
Build Security In - https://buildsecurityin.us-cert.gov
and SwA information clearinghouse – http://us-cert.gov/SwA
http://www.owasp.org/index.php/OWASP_CLASP_Project

Homeland Security

SwA Working Group Sessions ~ every two months
Next SwA Forum 14 – 16 Oct 2008, NIST HQ, Gaithersburg, MD

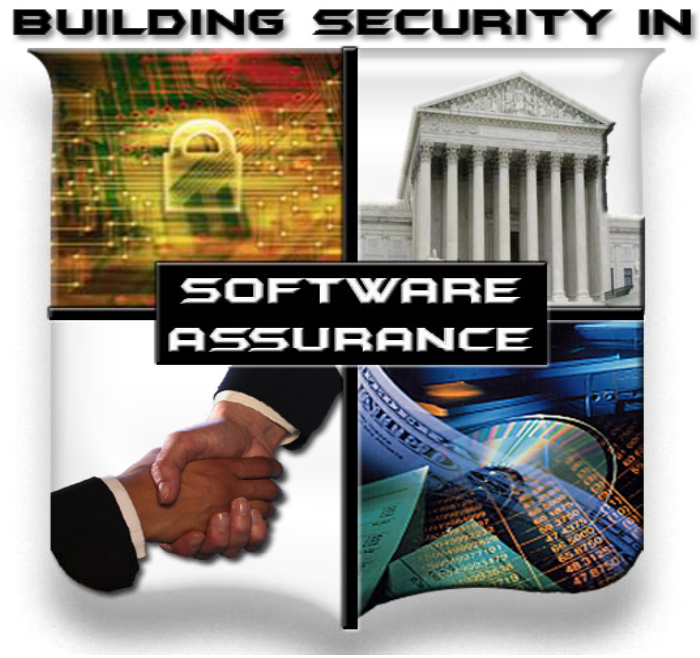
https://buildsecurityin.us-cert.gov/swa/
for SwA Community of Practice

http://buildsecurityin.us-cert.gov



Joe Jarzombek, PMP
Director for Software Assurance
National Cyber Security Division
Joe.Jarzombek@dhs.gov

Homeland Security

Homeland Security

Questions?