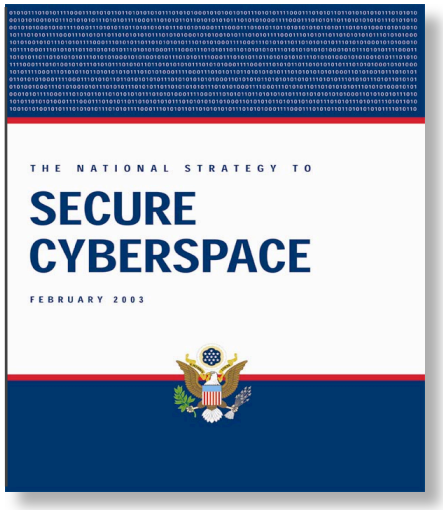
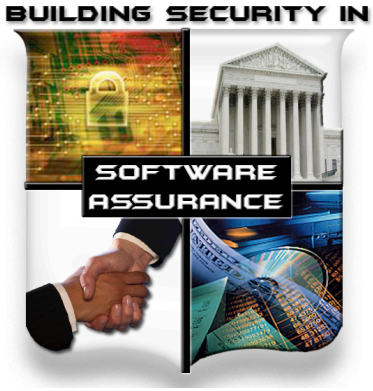
Software Assurance:

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



Mitigating Software Supply Chain Risks



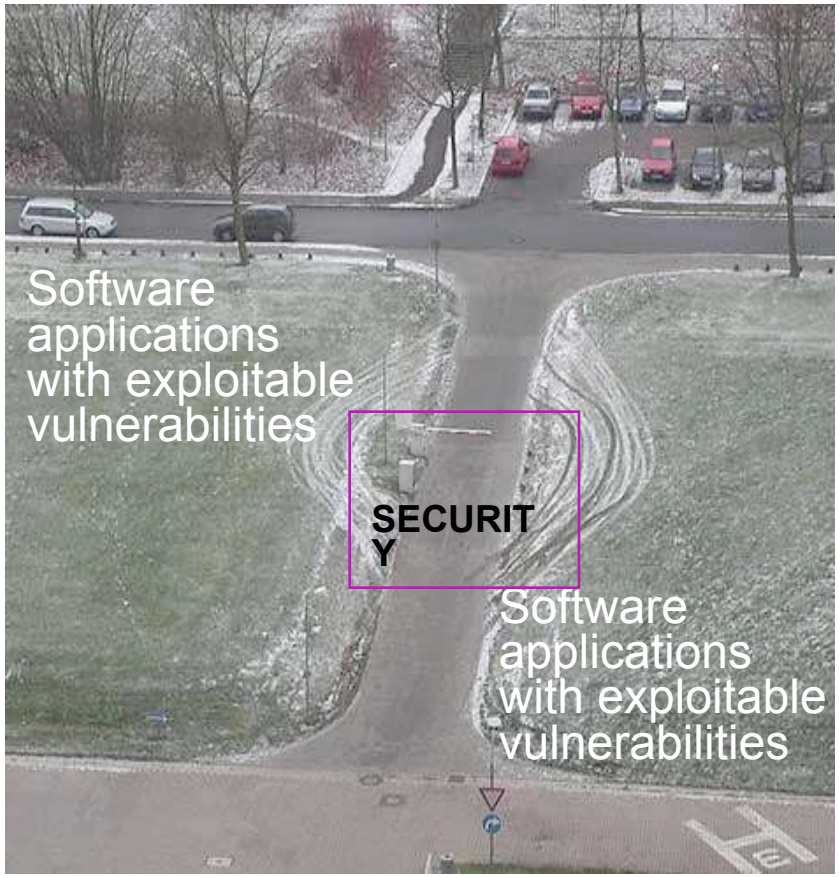
11 Dec 2008

Homeland Security

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

Security is a Requisite Quality Attribute: Vulnerable Software Enables Exploitation

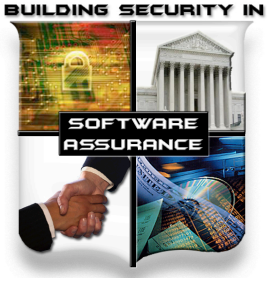
- Rather than attempt to break or defeat network or system security, hackers are opting to target application software to circumvent security controls.
  - **75% of hacks occurred at application level**
    - "90% of software attacks were aimed at application layer" (Gartner & Symantec, June 2006)
  - 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

Security-Enhanced Capabilities:
Mitigating Risks to the Enterprise



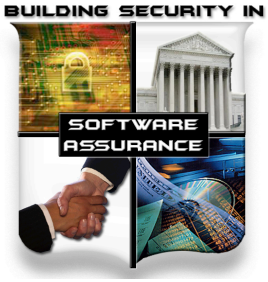
- With today's global software supply chain, Software Engineering, Quality Assurance, Testing and Project Management must explicitly address security risks posed by exploitable software.
  - Traditional processes do not explicitly address software-related security risks that can be passed from projects 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)

"Who Pushed Vendors Toward Better Security?"

CSO Magazine www.csoonline.com December 03, 2008



By Oracle Corp. CSO Mary Ann Davidson, December 03, 2008 -- Excerpts from article:

In the past five years, software assurance has moved from the theoretical to the practical, as more vendors disclose or are required to disclose their secure development practices if they are not actually trying to use these practices as competitive differentiators.

The market shift has been led by critical customer segments as much or more so than by a vendor awakening.

Customers are increasingly focused upon lifecycle security costs in part because unexpected security events have become a large and unpredictable part of organizations' IT budgets. …Customer demand is changing the marketplace for secure software, a trend that will accelerate through purchasing power or by policies with the effect of regulation.

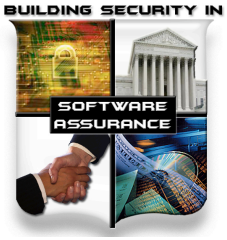
The US federal government is a significant player in changing the security marketplace.

…US federal agencies want more transparency regarding how, where and by whom the software they use is developed, in part to better assess risk, of which software security-worthiness is a large component.

…A number of US government agencies, including DoD, NSA, OMB and DHS, are focused on software security. DHS runs a software assurance forum where a broad tent of industry, academia and customers collaborate on better software development practices. Multiple DHS software assurance working groups have produced materials in areas as diverse as secure development practice, security metrics, acquisition and developer education.

Source: http://www.csoonline.com/article/467314/Who_Pushed_Vendors_Toward_Better_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 resources & info clearinghouse

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 Attribute & Enumeration (MAEC)

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.

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

Abuse Cases | Security Requirements | Risk Analysis | Design Review | Risk-based Test Plans | Code Review | Static Analysis | Risk Analysis | Penetration Testing | Security Ops & Vulnerability Mgt

Requirements and Use Cases | Architecture and Detailed Design | Code and Testing | Field Deployment and Feedback

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)

Fundamental Practices for Secure Software Development:
A Guide to the Most Effective Secure Development Practices in Use Today, Oct 8, 2008

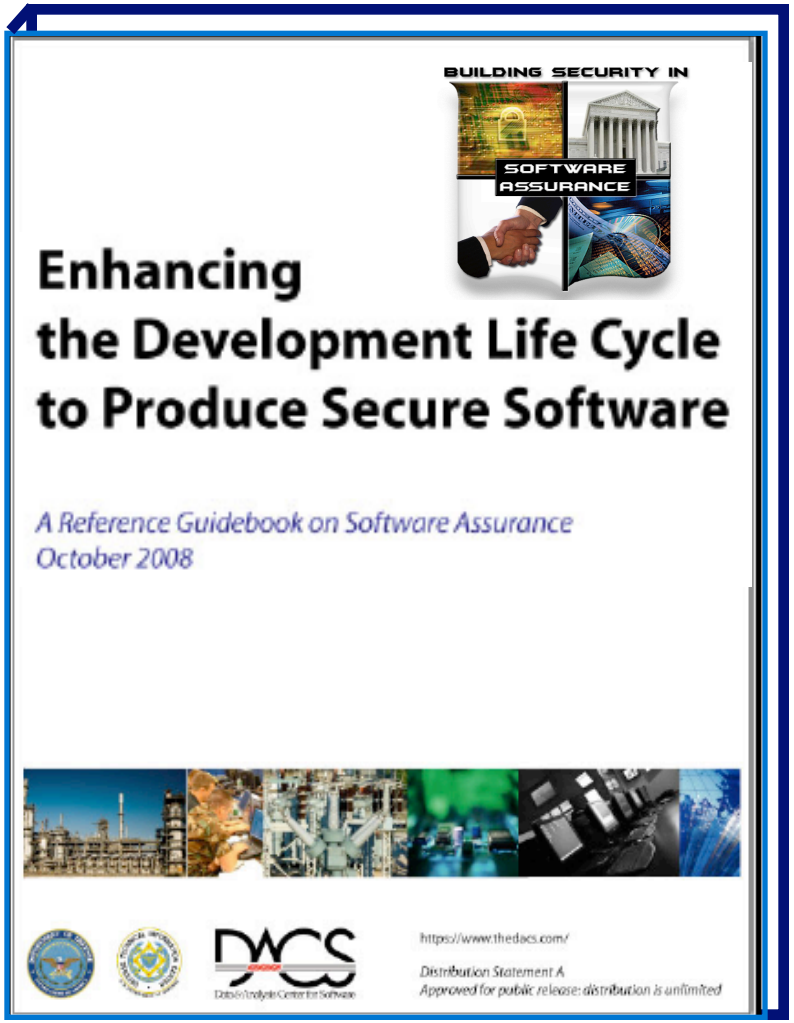
- Common security-related elements of software development methodologies
  - Security requirements help drive design, code handling, programming, and testing activities
- Secure Programming practices:
  - Minimize unsafe function use
  - Use the latest compiler toolset
  - Use static and dynamic analysis tools
  - Use manual code review on high-risk code
  - Validate input and output
  - Use anti-cross site scripting libraries
  - Use canonical data formats
  - Avoid string concatenation for dynamic SQL
  - Eliminate weak cryptography
  - Use logging and tracing
- Test to validate robustness and security
  - Fuzz testing
  - Penetration testing & third party assessment
  - Automated test tools (in all development stages)
- Code Integrity and Handling
  - Least privilege access, Separation of duties,
  - Persistent protection, Compliance management; Chain of custody & supply chain integrity.
- Documentation (about software security posture & secure configuration)

http://www.safecode.org/publications/SAFECode_Dev_Practices1108.pdf

Enhancing the Development Life Cycle to Produce Secure Software

A Reference Guidebook on Software Assurance, October 2008

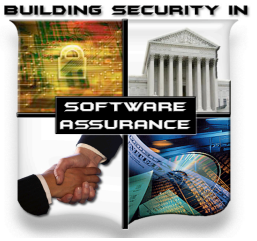
- Describes how to integrate security principles and practices in software development life cycle
- Addresses security requirements, secure design principles, secure coding, risk-based software security testing, and secure sustainment
- Provides guidance for selecting secure development methodologies, practices, and technologies
  - Collaboratively developed/updated via SwA Forum working groups
  - Released Oct 2008 by DACS
  - Free, available for download via DACS and DHS SwA CRIC



Homeland Security

https://www.thedacs.com/techs/enhanced_life_cycles/

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
  5. Secure software integration/assembly practices
  6. Security testing practices that focus on verifying S/W dependability, trustworthiness, & sustainability
  7. Secure distribution and deployment practices and mechanisms
  8. Secure sustainment practices
  9. Supportive security tools
  10. Secure software configuration management systems and processes
- 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].

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

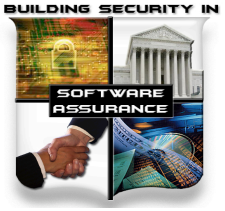
System
- Penetration testing
- Incident management
- Deployment & operations
- Black box testing
- Resources

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



Structuring Software Assurance CBK Content for Curricula Considerations

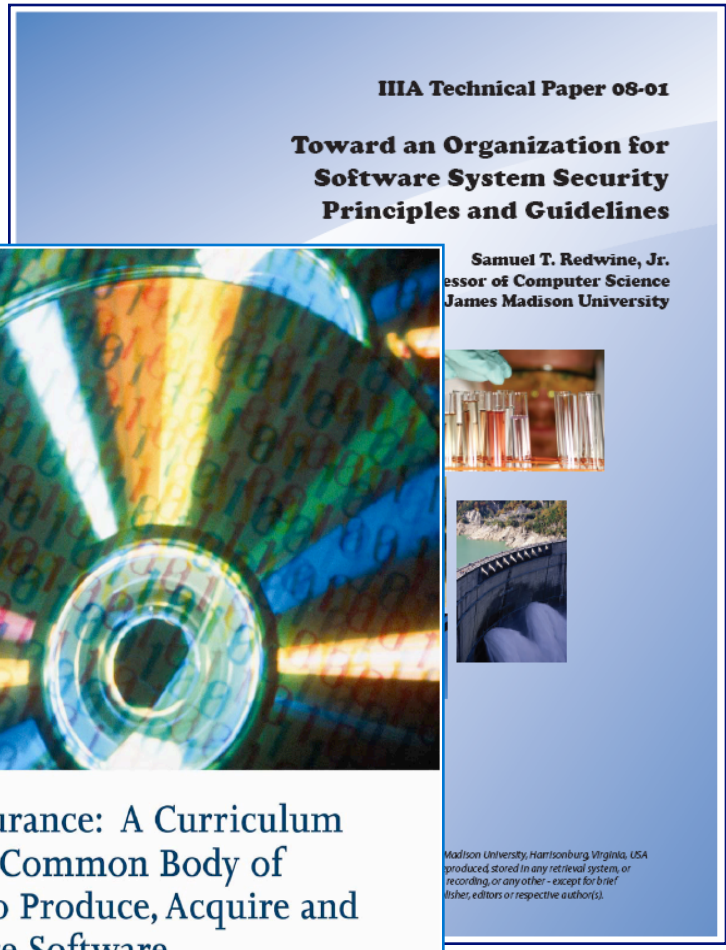
"Toward an Organization for Software System Security Principles and Guidelines,"
Version 1.0, IIIA Technical Paper 08-01. Feb 2008

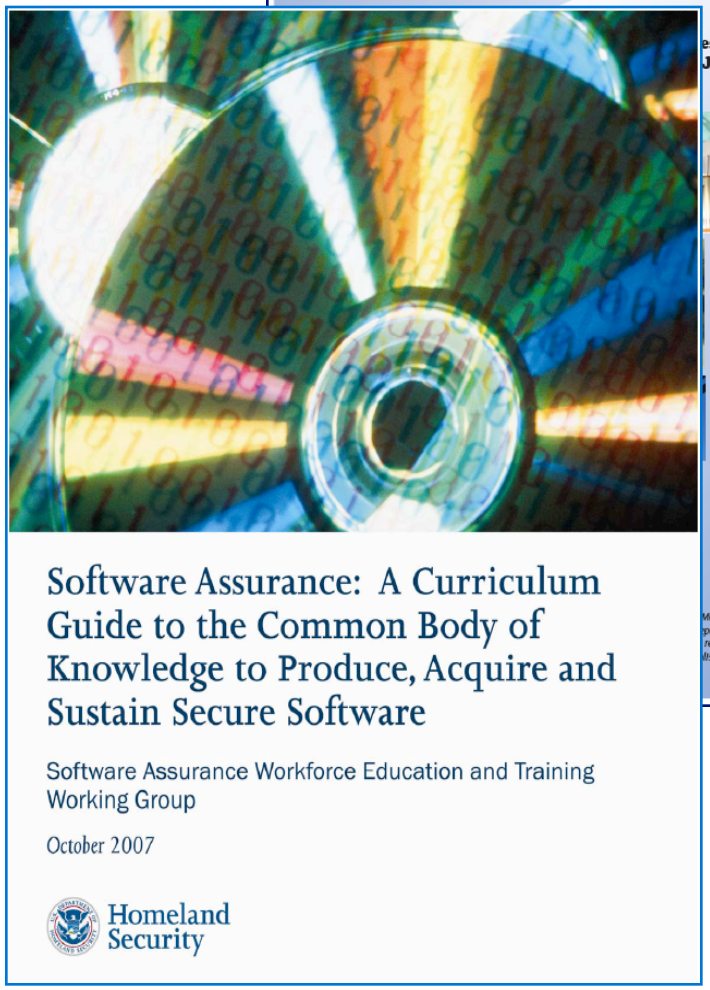
"Software Assurance: A Curriculum Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software,"
updated Oct 2007

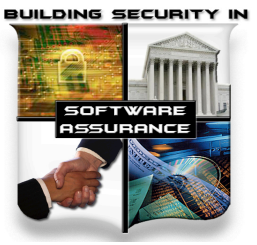
Both collaboratively developed through the Software Assurance Working Group on Workforce Education and Training
Co-chair Samuel T. Redwine, Jr.,

Institute for Infrastructure and Information Assurance,

James Madison University







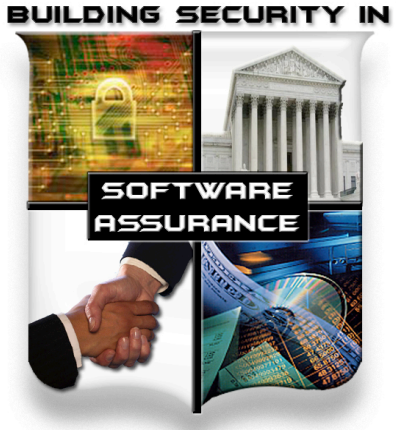
http://www.jmu.edu/iiia/webdocs/Reports/SwA_Principles_Organization-sm.pdf

Version 1.0, Oct 2008, published by National Defense University Press

Software Assurance in Acquisition: Mitigating Risks to the Enterprise

A Reference Guide for Security-Enhanced Software Acquisition and Outsourcing

October 22, 2008



Homeland Security

See https://buildsecurityin.us-cert.gov/swa/acqgde.html

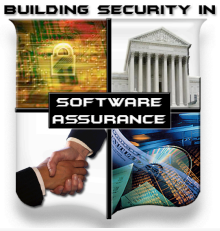
What if…

- **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;
  - Collaboratively advanced use of software security measurement & benchmarking schemes
  - Promoted use of methodologies and tools that enabled security to be part of normal business.
- **Acquisition managers & users factored risks posed by the software 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

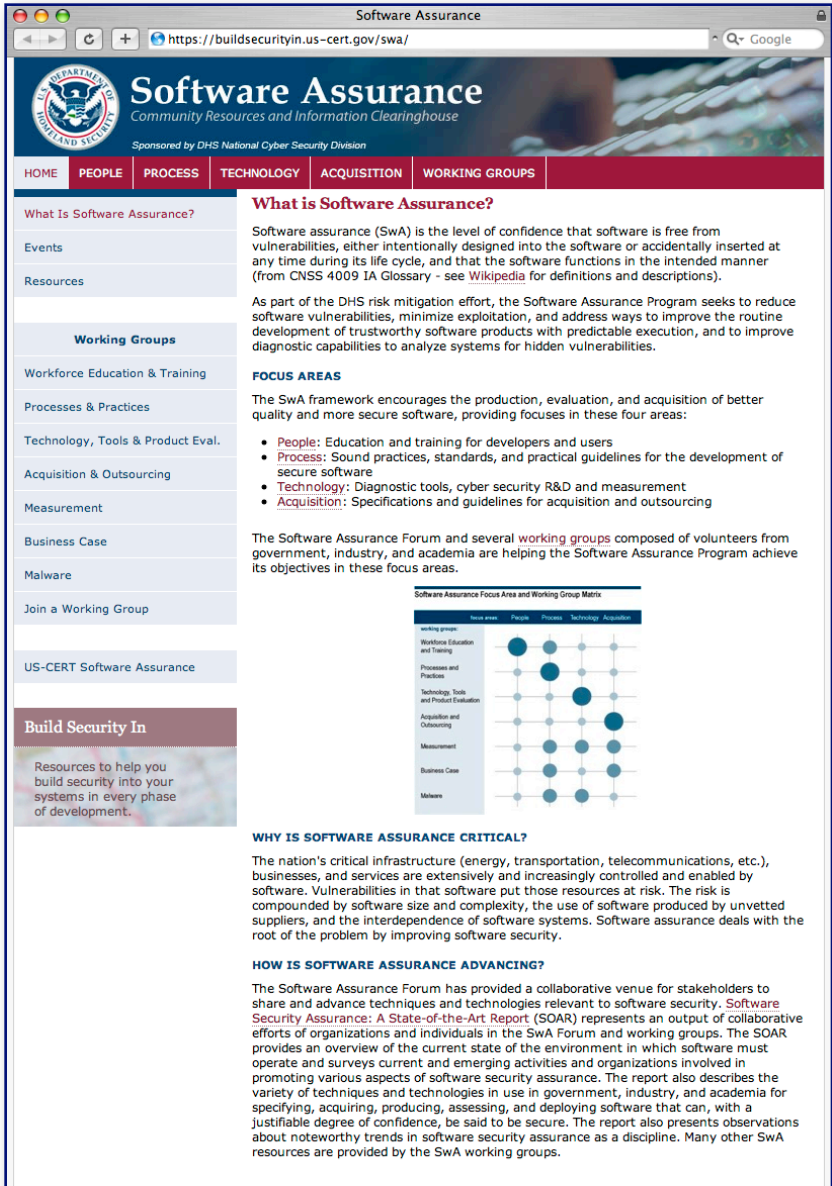
SwA Forum & Working Group Sessions – Next SwA Forum 10-12 March 2009

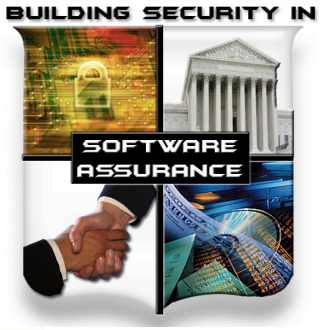


https://buildsecurityin.us-cert.gov/swa/
for SwA Community of Practice

https://buildsecurityin.us-cert.gov

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





SOFTWARE ASSURANCE FORUM

"Building Security In"

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

Homeland Security

Next SwA Forum 10-12 March 2009