

# Software Assurance

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



## Collaboratively Advancing Strategies to Mitigate Software Supply Chain Risks

30 July 2009



Homeland  
Security

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

# 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.*

- **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 to facilitate the adoption of Malware Attribute Enumeration Classification (MAEC), Common Weakness Enumeration (CWE), and Common Attack Pattern Enumeration and Classification (CAPEC).



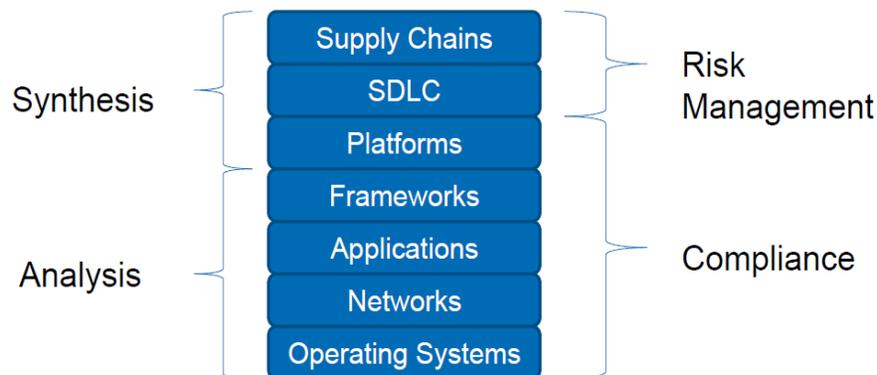
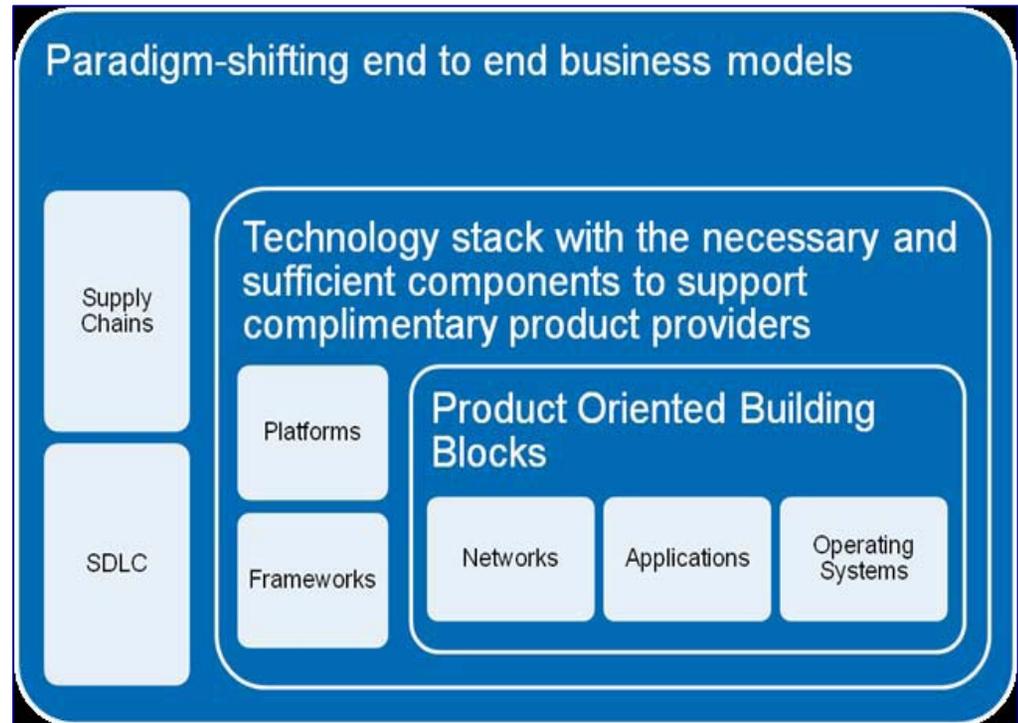
# IT/software security risk landscape is a convergence between “defense in depth” and “defense in breadth”

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.”

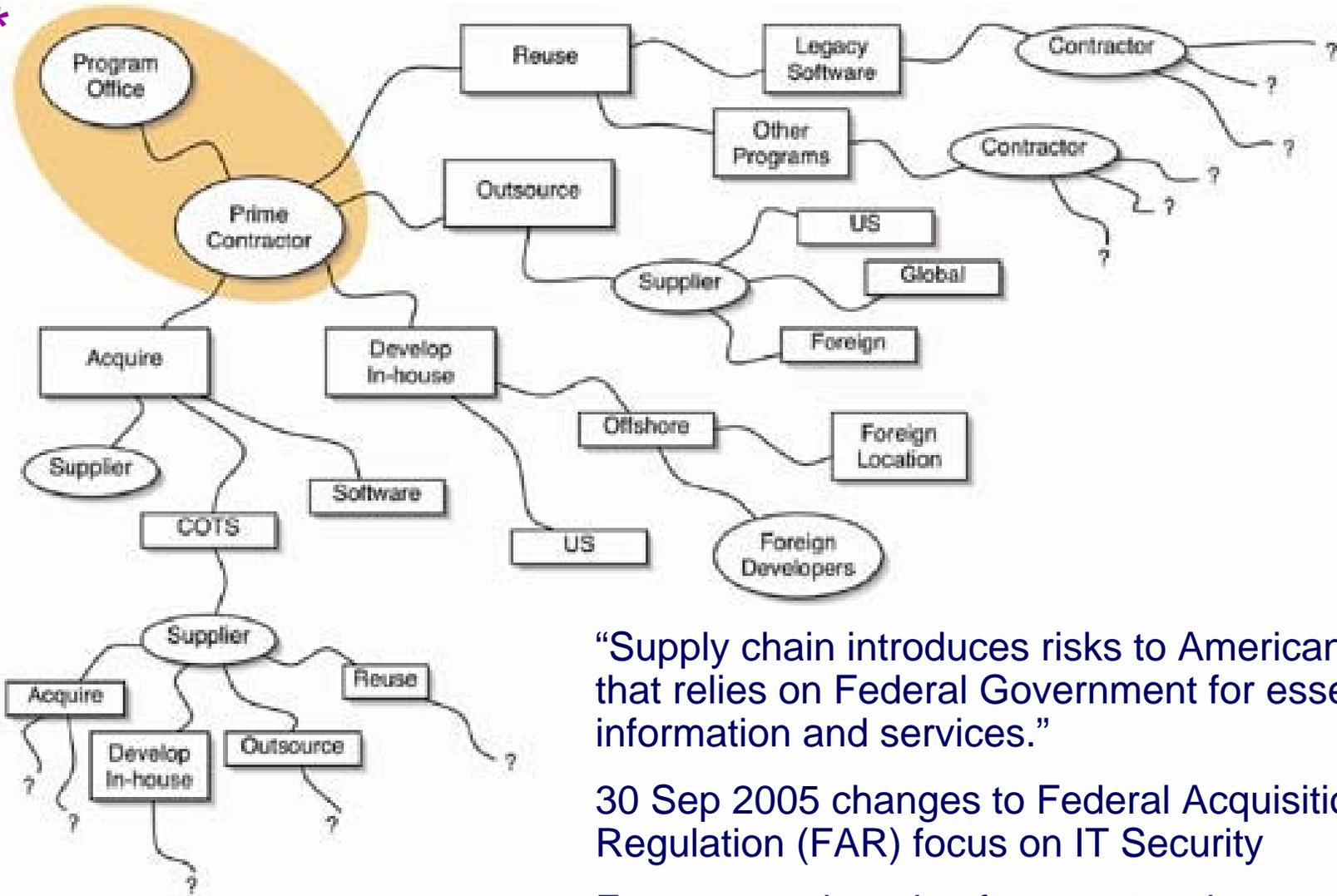
– Dan Geer, CISO In-Q-Tel



Software Assurance provides a focus for:

- Secure Software Components,
- Security in the SDLC and
- Software Supply Chain Risk Management

\*



“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.

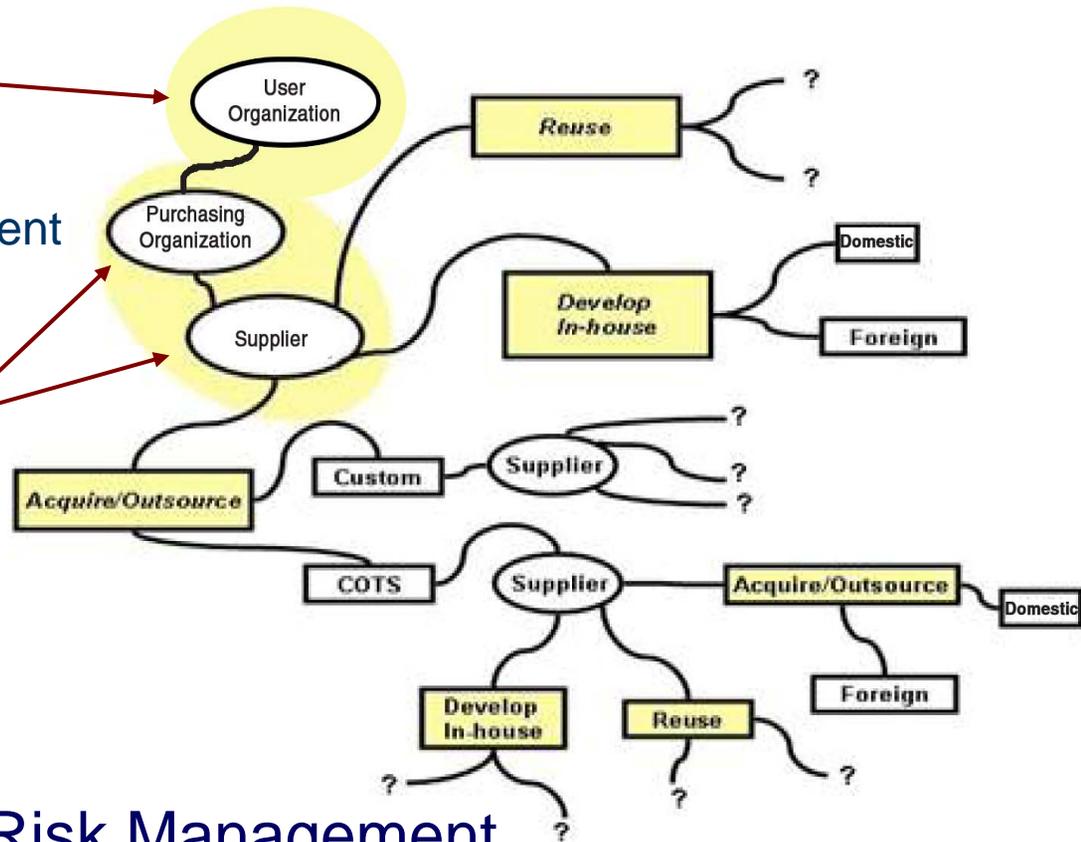
# Risk Management (Enterprise $\Leftrightarrow$ Project): Shared Processes & Practices // Different Focuses

## ► 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

# 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.

# Software Assurance “End State” Objectives...

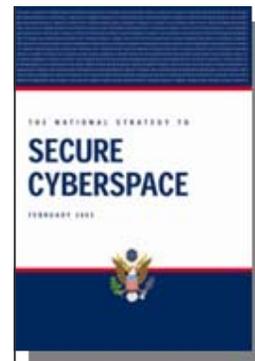
- ▶ **Government, in collaboration with industry / academia, raised expectations for product assurance with requisite levels of integrity and security:**
  - Helped advance more comprehensive software assurance diagnostic capabilities to mitigate risks stemming from exploitable vulnerabilities and weaknesses;
  - 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.



# DHS Software Assurance Program Overview

- ▶ Program established in response to 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 and resilience** of software across the development, acquisition, and operational life cycle
- ▶ DHS Software Assurance (SwA) program is scoped to address:
  - **Trustworthiness** - No exploitable vulnerabilities or malicious logic exist in the software, either intentionally or unintentionally inserted,
  - **Dependability (Correct and Predictable Execution)** - Justifiable confidence that software, when executed, functions as intended,
  - **Survivability** - If compromised, damage to the software will be minimized, and it will recover quickly to an acceptable level of operating capacity;
  - **Conformance** – Planned, systematic set of multi-disciplinary activities that ensure processes/products conform to requirements, standards/procedures.



# 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

<p>Build Security In - <a href="https://buildsecurityin.us-cert.gov">https://buildsecurityin.us-cert.gov</a> and SwA community resources &amp; info clearinghouse</p> <p>SwA Common Body of Knowledge (CBK) &amp; Glossary            Organization of SwSys Security Principles/Guidelines            SwA Developers' Guide on Security-Enhancing SDLC</p> <p>Software Security Assurance State of the Art Report            Systems Assurance Guide (via DoD and NDIA)</p> <p>SwA-related standards – ISO/IEC JTC1 SC7/27/22, IEEE CS, OMG, TOG, &amp; CMM-based Assurance</p>	<p>Practical Measurement Framework for SwA/InfoSec            Making the Business Case for Software Assurance</p> <p>SwA Metrics &amp; Tool Evaluation (with NIST)            SwA Ecosystem w/ DoD, NSA, NIST, OMG &amp; TOG            NIST Special Pub 500 Series on SwA Tools</p> <p>Common Weakness Enumeration (CWE) dictionary            Common Attack Pattern Enumeration (CAPEC)</p> <p>SwA in Acquisition: Mitigating Risks to Enterprise Software Project Management for SwA SOAR</p>
---	--



\* 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.

# SwA Collaboration for Content & Peer Review



## Build Security In

*Setting a higher standard for software assurance*

*Sponsored by DHS National Cyber Security Division*

BSI <https://buildsecurityin.us-cert.gov> focuses with a thrust to make Software Security a normal part of Software Engineering



## Software Assurance

*Community Resources and Information Clearinghouse*

*Sponsored by DHS National Cyber Security Division*

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 FORUM

## BUILDING SECURITY IN

### *Business Case for Software Assurance*

April 2009 SwA Report provides background, context and examples:

- Motivators
- Cost/Benefit Models Overview
- Measurement
- Risk
- Prioritization
- Process Improvement & Secure Software
- Globalization
- Organizational Development
- Case Studies and Examples

 Software Engineering Institute

### Making the Business Case for Software Assurance

Nancy R. Mead  
Julia H. Allen  
W. Arthur Conklin  
Antonio Drommi  
John Harrison  
Jeff Ingalsbe  
James Rainey  
Dan Shoemaker

April 2009

**SPECIAL REPORT**  
CMU/SEI-2009-SR-001

**CERT Program**  
Unlimited distribution subject to the copyright.

<http://www.sei.cmu.edu>



Carnegie Mellon



# SOFTWARE ASSURANCE FORUM

## BUILDING SECURITY IN

### Security Measurement Resources

Oct 2008 → May 2009 →

### Practical Measurement Framework for Software Assurance and Information Security

Oct 2008



### The Center for Internet Security

### The CIS Security Metrics

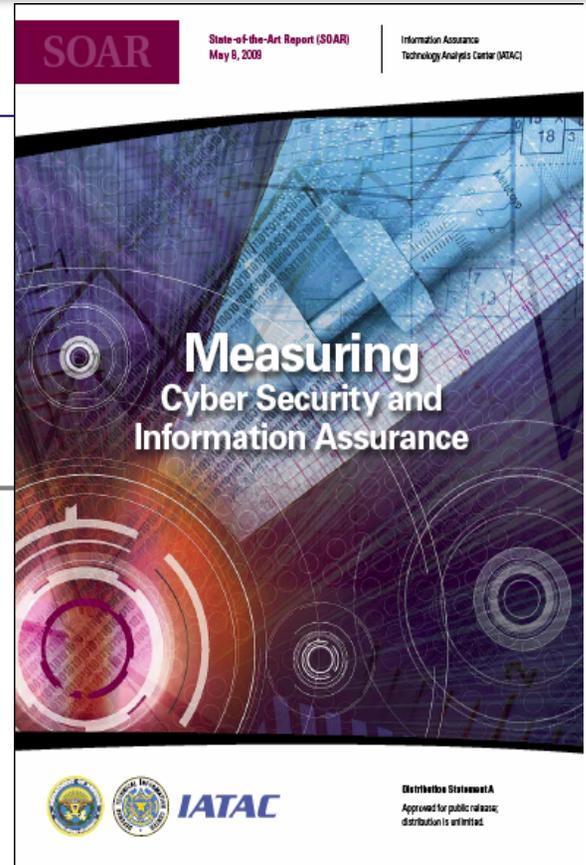
February 9

# 2009

Organizations struggle to make cost-effective security investment decisions; information security professionals lack widely accepted and unambiguous metrics for decision support. CIS established a consensus team of one hundred (100) industry experts to address this need. The result is a set of standard metric and data definitions that can be used across organizations to collect and analyze data on security process performance and outcomes.

This document contains twenty-one (21) metric definitions for six (6) important business functions: Incident Management, Vulnerability Management, Patch Management, Application Security, Configuration Management and Financial Metrics. Additional consensus metrics are currently being defined for these and additional business functions.

Consensus Metric Definitions





# SOFTWARE ASSURANCE FORUM BUILDING SECURITY IN

*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

## Executive Summary

### 1. Introduction

- 1.1 Background
- 1.2 Purpose and Scope
- 1.3 Audience—Acquisition Official Defined
- 1.4 Document Structure
- 1.5 Risk-Managed Software Acquisition Process

### 2. Planning Phase

- 2.1 Needs Determination, Risk Categorization, & Solution Alternatives
- 2.2 SwA Requirements
- 2.3 Acquisition Plan and/or Acquisition Strategy
- 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
- 3.4 Contract Award

### 4. Implementation and Acceptance Phase

- 4.1 Contract Work Schedule
- 4.2 Change Control
- 4.3 Risk Management Plan
- 4.4 Assurance Case Management
- 4.5 Independent Software Testing
- 4.6 Software Acceptance

### 5. Follow-on Phase

- 5.1 Support and Maintenance
  - 5.1.1 Risk Management
  - 5.1.2 Assurance Case Management—Transition to Ops
  - 5.1.3 Other Change Management Considerations
- 5.2 Disposal or Decommissioning

### Appendix A/B— Acronyms/Glossary

### Appendix C— An Imperative for SwA in Acquisition

### Appendix D— Software Due Diligence Questionnaires

- Table D-1. COTS Proprietary Software Questionnaire
- Table D-2. COTS 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 Commercial Software
- F.3 Acceptance Criteria
- F.4 Certifications
- F.5 Sample Instructions to Offerors Sections
- F.6 Sample Work Statement Sections
- F.7 Open Web Application Security Project
- F.8 Certification of Originality

### Appendix H— References



# Software Assurance (SwA) Pocket Guide Series

## SwA in Acquisition & Outsourcing

- Contract Language for Integrating Software Security into the Acquisition Life Cycle
- 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

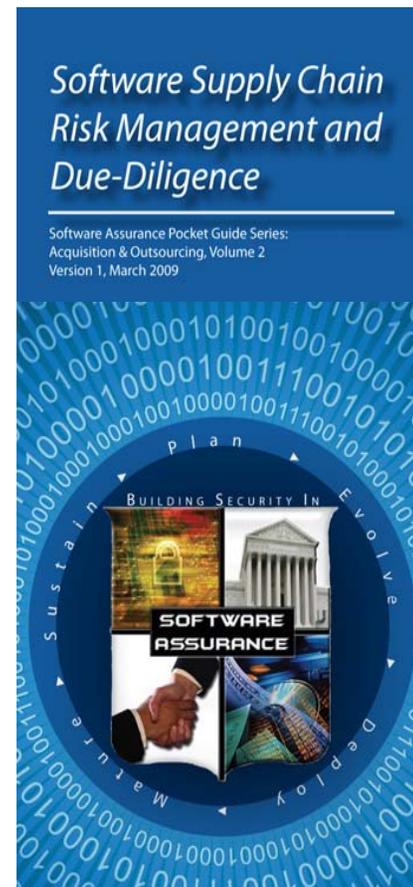
## SwA Life Cycle Support

- 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)



<b>SwA Concern Categories</b>	<b>Risks</b>	<b>Purpose for Questions</b>
<p><b>Software History and Licensing</b>  <b>Development Process Management</b>  <b>Software Security Training and Planning and Requirements</b>  <b>Architecture and Design</b>  <b>Software Development</b>  <b>Built-in Software Defenses</b>  <b>Component Assembly</b>  <b>Testing</b>  <b>Software Manufacture and Packaging</b>  <b>Installation</b>  <b>Assurance Claims and Evidence</b>  <b>Support</b>  <b>Software Change Management</b>  <b>Timeliness of Vulnerability Mitigation</b>  <b>Individual Malicious Behavior</b>  <b>Security “Track Record”</b>  <b>Financial History and Status</b>  <b>Organizational History</b>  <b>Foreign Interests and Influences</b>  <b>Service Confidentiality Policies</b>  <b>Operating Environment for Services</b>  <b>Security Services and Monitoring</b></p>		

**Table 1 – SwA Concern Categories -- (with interests relevant to security and privacy)**

SwA Concern Categories	Risks	Purpose for Questions
<b>Service Confidentiality Policies</b>	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
<b>Service Confidentiality Policies</b>	
<b>1</b>	What are the customer confidentiality policies? How are they enforced?
<b>2</b>	What are the customer privacy policies? How are they enforced?
<b>3</b>	What are the policies and procedures used to protect sensitive information from unauthorized access? How are the policies enforced?
<b>4</b>	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?
<b>Operating Environment for Services</b>	
<b>5</b>	Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all registry settings?
<b>7</b>	What are the data backup policies and procedures? How frequently are the backup procedures verified?
<b>11</b>	What are the agents or scripts executing on servers of hosted applications? Are there procedures for reviewing the security of these scripts or agents?
<b>12</b>	What are the procedures and policies used to approve, grant, monitor and revoke access to the servers? Are audit logs maintained?
<b>13</b>	What are the procedures and policies for handling and destroying sensitive data on electronic and printed media?
<b>15</b>	What are the procedures used to approve, grant, monitor, and revoke file permissions for production data and executable code?



# National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

## National Vulnerability Database (NVD) Version 2.2 -- <http://nvd.nist.gov/>

- ▶ NVD is the U.S. government repository of standards based vulnerability management data represented using the [Security Content Automation Protocol](#) (SCAP).
- ▶ This data enables automation of vulnerability management, security measurement, & compliance.
- ▶ NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics. NVD supports the [Information Security Automation Program](#).

## Federal Desktop Core Configuration settings (FDCC)

- ▶ NVD contains content (and pointers to tools) for performing configuration checking of systems implementing the [FDCC](#) using the Security Content Automation Protocol ([SCAP](#)).
- ▶ [FDCC Checklists](#) are available to be used with [SCAP FDCC Capable Tools](#) -- available via NVD.

## NVD Primary Resources

- ▶ [Vulnerability Search Engine](#) (CVE software flaws and CCE misconfigurations)
- ▶ [National Checklist Program](#) (automatable security configuration guidance in XCCDF and OVAL)
- ▶ [SCAP](#) (program and protocol that NVD supports) and [SCAP Compatible Tools](#)
- ▶ [SCAP Data Feeds](#) (CVE, CCE, CPE, CVSS, XCCDF, OVAL)
- ▶ [Product Dictionary](#) (CPE) and [Impact Metrics](#) (CVSS)
- ▶ [Common Weakness Enumeration](#) (CWE)

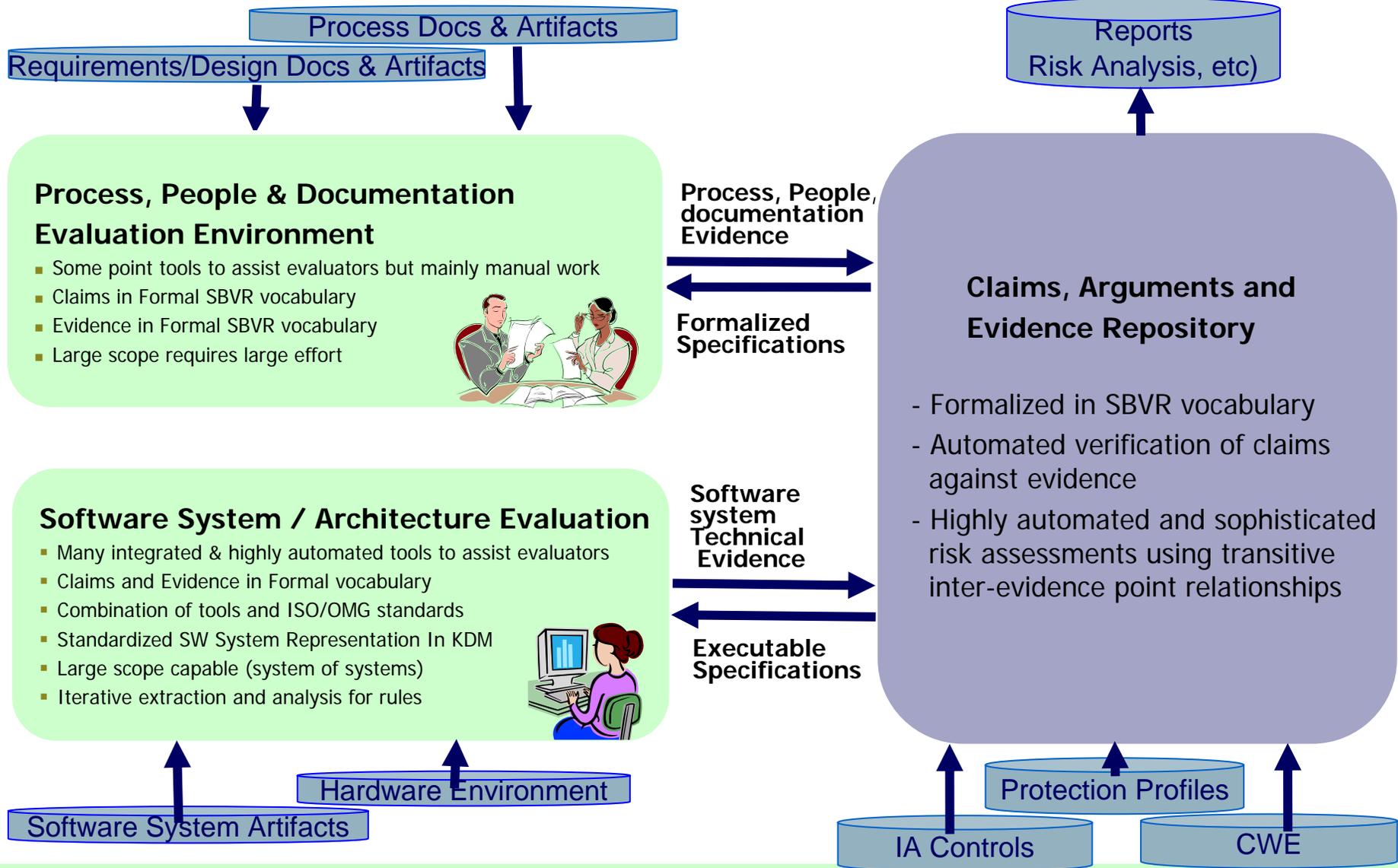
# Standard Enumerations for Addressing Common Weaknesses and Common Attack Patterns



- ▶ DHS NCSD Software Assurance program co-sponsors the Common Weakness Enumeration (CWE) [<http://cwe.mitre.org/>] and the Common Attack Pattern Enumeration and Classification (CAPEC) [<http://capec.mitre.org/>]
  - To more effectively understand their risk exposure, consumers need to understand exploitable weaknesses in software before put into use and throughout the lifecycle.
  - These are standard enumerations and community knowledge resources.
  - These enable consumers to be better informed about the resilience and security of software we acquire and use.
- ▶ As a standard enumeration, CWE provides a unified, measurable set of exploitable software weaknesses that now enables more effective discussion, description, selection and use of software security tools and services that can find these weaknesses in source code (with one intent to discover them before the code is put into use).

# Software Assurance Ecosystem: The Formal Framework

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



SWA processes & practices are moving toward more disciplined, less subjective with more automated, comprehensive tooling and formalized specifications

# Software Supply Chain Management is a National Security Issue

- ▶ Adversaries can gain “intimate access” to target systems, especially in a global supply chain that offers limited transparency
- ▶ Advances in computer 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
- ▶ 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

Globalization will not be reversed;  
this is how we conduct business

# Next SwA Forum 2-6 Nov 2009 in the Washington DC metro area

## Next SwA Working Group Session 15-17 Dec 2009 at MITRE, McLean VA

### SwA Community Resources & Information Clearinghouse

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

Build Security In web site

<https://buildsecurityin.us-cert.gov>

**Build Security In**  
Sponsored by DHS National Cyber Security Division

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

Login: Username:  Password:

Quick Search:

### Articles

What's New  
Top Viewed Articles

Articles by Category

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

### Knowledge

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

### Tools

- Black Box Testing
- Code Analysis
- Modeling Tools

### Featured Forums

#### Getting Started with Build Security In

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

**Architectures & Design**

- Architectural risk analysis
- Process modeling
- Principles
- Guidelines
- Historical risks
- Modeling tools
- Resources

**Code**

- Code review
- Security, integrations, & evolution
- Coding practices
- Coding rules
- Code analysis
- Resources

**Test**

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

**Requirements**

- Requirement engineering
- Attack patterns
- Resources

**System**

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

**Key**

- Best practices
- Foundational knowledge
- Tools
- Resources

#### What is "Build Security In" (BSI)?

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

#### How Can I Collaborate?

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

#### What's New

##### Source Code Analysis Tools - Overview

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

[Source Code Analysis Tools ? Business Case](#)

**Software Assurance**  
Community Resources and Information Clearinghouse

Sponsored by DHS National Cyber Security Division

HOME | PEOPLE | PROCESS | TECHNOLOGY | ACQUISITION | WORKING GROUPS

### What is Software Assurance?

Software assurance (SwA) is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at 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.

### Working Groups

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

Join a Working Group

US-CERT Software Assurance

### Build Security In

Resources to help you build security into your systems in every phase of development.

#### Software Assurance Focus Area and Working Group Matrix

Working Group	Focus Area	People	Process	Technology	Acquisition
Workforce Education and Training	People	●	●	●	●
Processes and Practices	Process	●	●	●	●
Technology, Tools and Product Evaluation	Technology	●	●	●	●
Acquisition and Outsourcing	Acquisition	●	●	●	●
Measurement	Measurement	●	●	●	●
Business Case	Business Case	●	●	●	●
Malware	Malware	●	●	●	●

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



#### 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 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. The report also describes the variety of techniques and technologies in use in government, industry, and academia for specifying, acquiring, producing, assessing, and deploying software that can, with a justifiable degree of confidence, be said to be secure. The report also presents observations about noteworthy trends in software security assurance as a discipline. Many other SwA resources are provided by the SwA working groups.

Next SwA Forum 2-6 Nov 2009 in the Washington DC metro area  
Next SwA Working Group Session 15-17 Dec 2009 at MITRE, McLean VA



# SOFTWARE ASSURANCE FORUM

“Building Security In”

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



Homeland  
Security

**BACK UP SLIDES**



## Process Agnostic Lifecycle

### 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

### Fundamentals

- ✓ Risk management
- ✓ Project management
- ✓ Training & awareness
- ✓ Measurement
- 🔍 SDLC process
- 🔍 Business relevance
- 📄 Resources

### System

- ✓ Penetration testing
- ✓ Incident management
- ✓ Deployment & operations
- 🔧 Black box testing
- 📄 Resources

### Key

- ✓ Best (sound) practices
- 🔍 Foundational knowledge
- 🔧 Tools
- 📄 Resources

<https://buildsecurityin.us-cert.gov>



Homeland Security



# Software Assurance

Community Resources and Information Clearinghouse

Sponsored by DHS National Cyber Security Division

[HOME](#)
[EVENTS](#)
[SWA MULTIMEDIA](#)
[SWA RESOURCES](#)

[GO](#) [customize](#)

## SwA Working Groups

[Workforce Education & Training](#)
[Processes & Practices](#)
[Technology, Tools & Product Eval.](#)
[Acquisition & Outsourcing](#)
[Measurement](#)
[Business Case](#)
[Malware Attribution](#)

## Join a SwA Working Group

## SwA Forums

## SwA Landscape

## 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 DHS risk mitigation efforts to enable greater resilience of cyber assets, the [Software Assurance Program](#) seeks to reduce software vulnerabilities, minimize exploitation, and address ways to routinely acquire, develop and deploy reliable and trustworthy software products with predictable execution, and to improve diagnostic capabilities to analyze systems for exploitable weaknesses.

The **Software Assurance Forum** and several **working groups**, composed of stakeholders in government, industry, and academia, are contributing to efforts focused on advancing software assurance objectives. The next Software Assurance Forum is ~~in October 2009~~ **2-6 Nov 2009**

Focused efforts for advancing software assurance are addressed in the working groups listed below. Click on any working group's name to see **Recent Releases and Updates**, current activities, and other information for that working group.

- [Workforce Education & Training](#)
- [Processes & Practices](#)
- [Technology, Tools & Product Evaluation](#)
- [Acquisition & Outsourcing](#)
- [Measurement](#)
- [Business Case](#)
- [Malware Attribution](#)

## BUILDING SECURITY IN



## WHY IS SOFTWARE ASSURANCE CRITICAL?

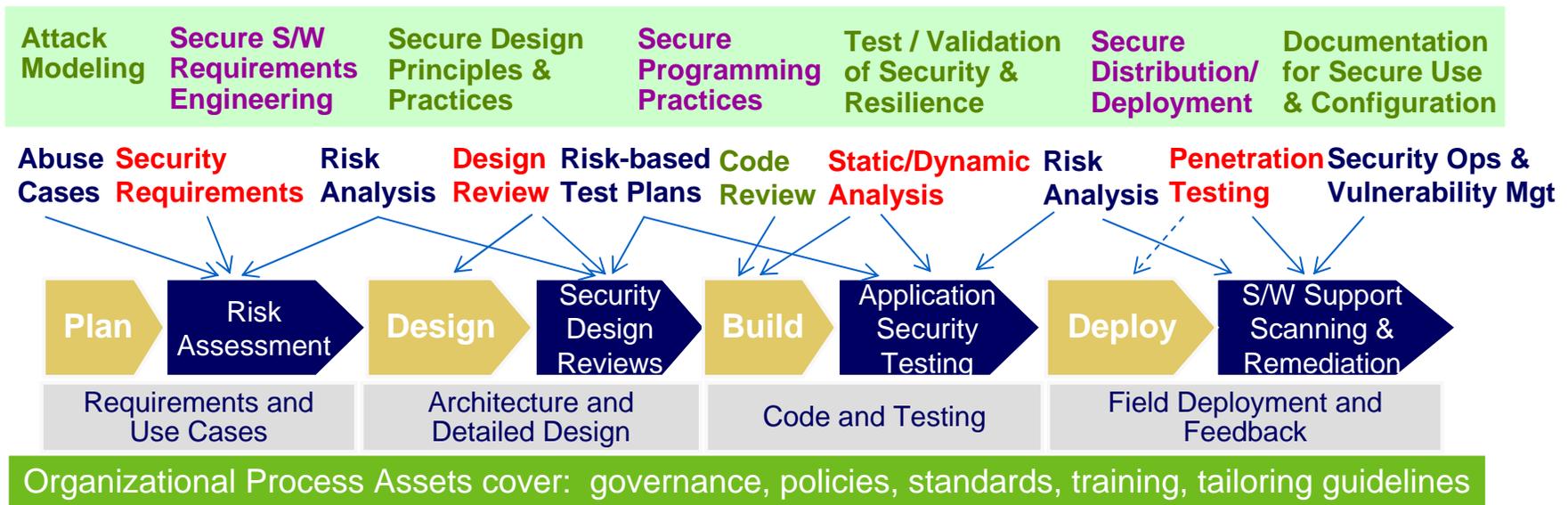
The nation's critical infrastructure (energy, transportation, telecommunications, etc.), businesses, and services are extensively and increasingly controlled and enabled by

See <https://buildsecurityin.us-cert.gov/swa/> for information

# Security-Enhanced Process Improvements

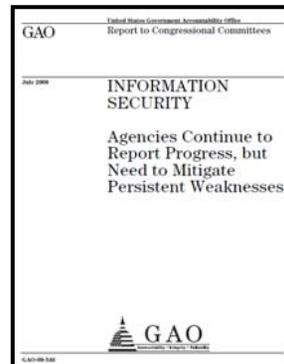
Organizations that provide security engineering & risk-based analysis throughout the lifecycle will have more resilient software products / systems.

“Build Security In” throughout the lifecycle



- ▶ 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.

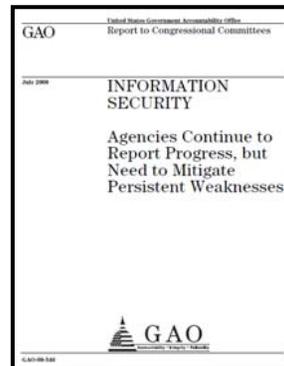
# July 2009 GAO Report on INFORMATION SECURITY: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses (GAO-09-546)



## What the Government Accountability Office Reported:

- Persistent weaknesses in information security policies and practices continue to threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of most federal agencies.
- Recently reported incidents at federal agencies have placed sensitive data at risk, including the theft, loss, or improper disclosure of personally identifiable information of Americans, thereby exposing them to loss of privacy and identity theft.
- For fiscal year 2008, almost all 24 major federal agencies had weaknesses in information security controls.
  - An underlying reason for these weaknesses is that agencies have not fully implemented their information security programs.
  - As a result, agencies have limited assurance that controls are in place and operating as intended to protect their information resources, thereby leaving them vulnerable to attack or compromise.
- In prior reports, GAO has made hundreds of recommendations to agencies for actions necessary to resolve prior significant control deficiencies and information security program shortfalls.

# July 2009 GAO Report on INFORMATION SECURITY: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses (GAO-09-546)



Included recommendations of March 2009 meeting of security experts on how to improve national the nation's cybersecurity strategy and posture:

- Develop a national strategy that clearly articulates strategic objectives, goals and priorities.
- Establish White House responsibility and accountability for leading and overseeing national cybersecurity policy.
- Establish a governance structure for strategy implementation.
- Publicize and raise awareness about the seriousness of the cybersecurity problem.
- Create an accountable, operational cybersecurity organization.
- Focus more actions on prioritizing assets and functions, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans.
- Bolster public/private partnerships through an improved value proposition and use of incentives.
- Focus greater attention on addressing the global aspects of cyberspace.
- Improve law enforcement efforts to address malicious activities in cyberspace.
- Place greater emphasis on cybersecurity research and development, including consideration of how to better coordinate government and private-sector efforts.
- Increase the cadre of cybersecurity professionals.
- **Make the federal government a model for cybersecurity, including using its acquisition function to enhance cybersecurity aspects of products and services.**
  - *The strategy establishes securing the government's cyber space as a key priority and advocates using federal acquisition to accomplish this goal.*
  - Although the federal government has taken steps to improve the cyber security of agencies (e.g., beginning to implement the CNCI initiatives), the GAO panel of experts indicated it still is not a model for cyber security; it has not made changes in its acquisition function and the training of government officials in a manner that effectively improves the cyber security capabilities of products and services purchased and used by federal agencies