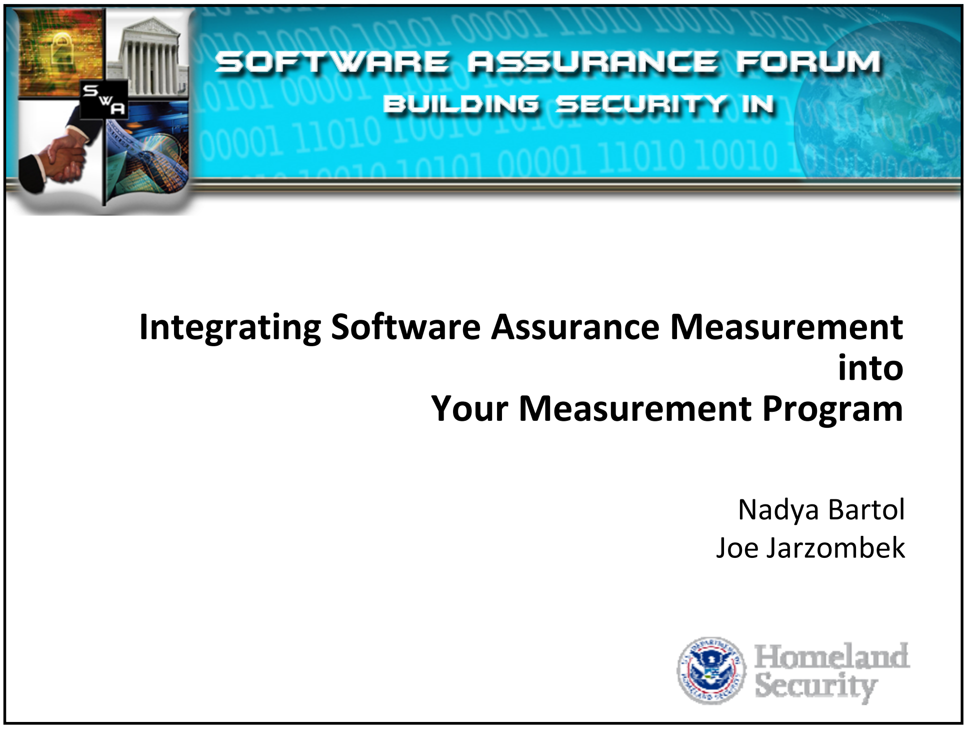


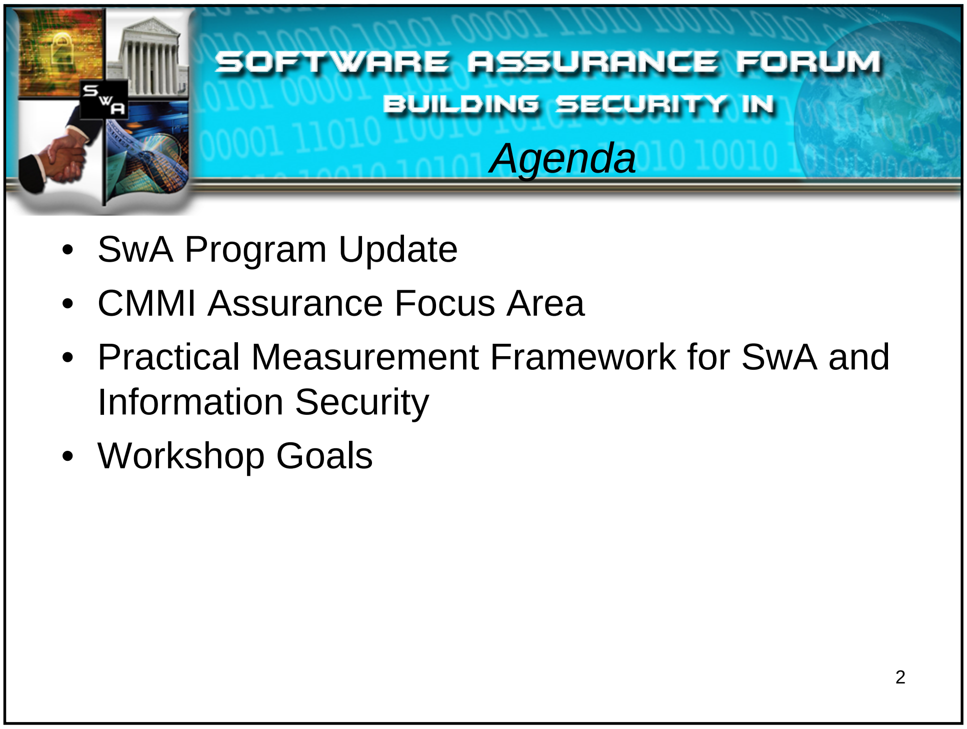
SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Integrating Software Assurance Measurement into Your Measurement Program

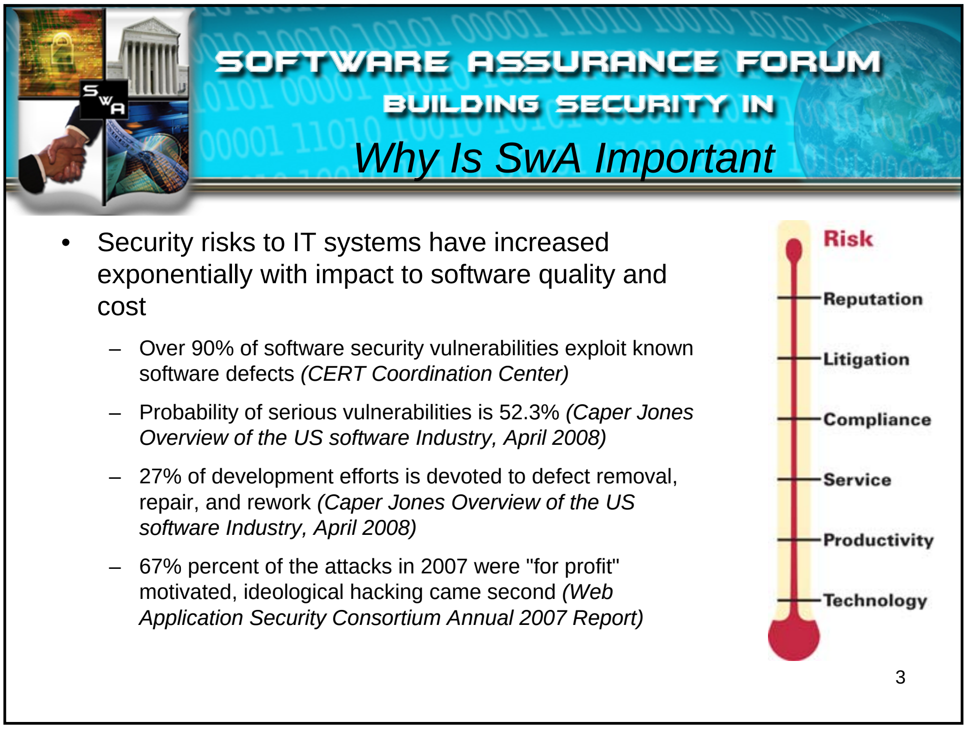
Nadya Bartol
Joe Jarzombek

Homeland Security



Agenda

- SwA Program Update
- CMMI Assurance Focus Area
- Practical Measurement Framework for SwA and Information Security
- Workshop Goals

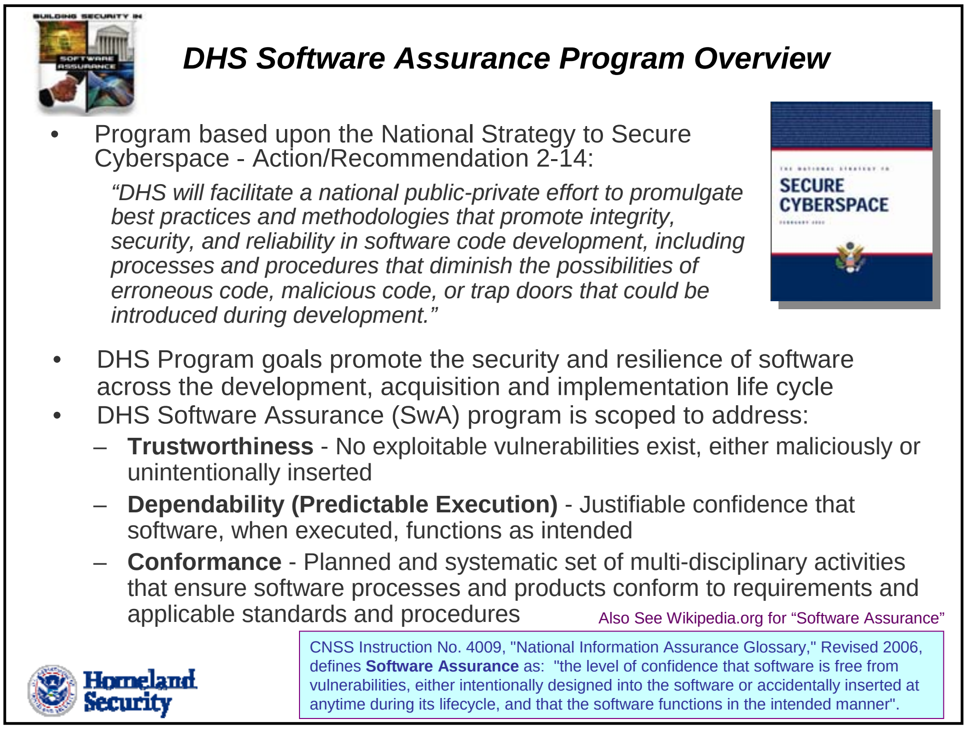


SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Why Is SwA Important

- Security risks to IT systems have increased exponentially with impact to software quality and cost
  - Over 90% of software security vulnerabilities exploit known software defects *(CERT Coordination Center)*
  - Probability of serious vulnerabilities is 52.3% *(Caper Jones Overview of the US software Industry, April 2008)*
  - 27% of development efforts is devoted to defect removal, repair, and rework *(Caper Jones Overview of the US software Industry, April 2008)*
  - 67% percent of the attacks in 2007 were "for profit" motivated, ideological hacking came second *(Web Application Security Consortium Annual 2007 Report)*



DHS Software Assurance Program Overview

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

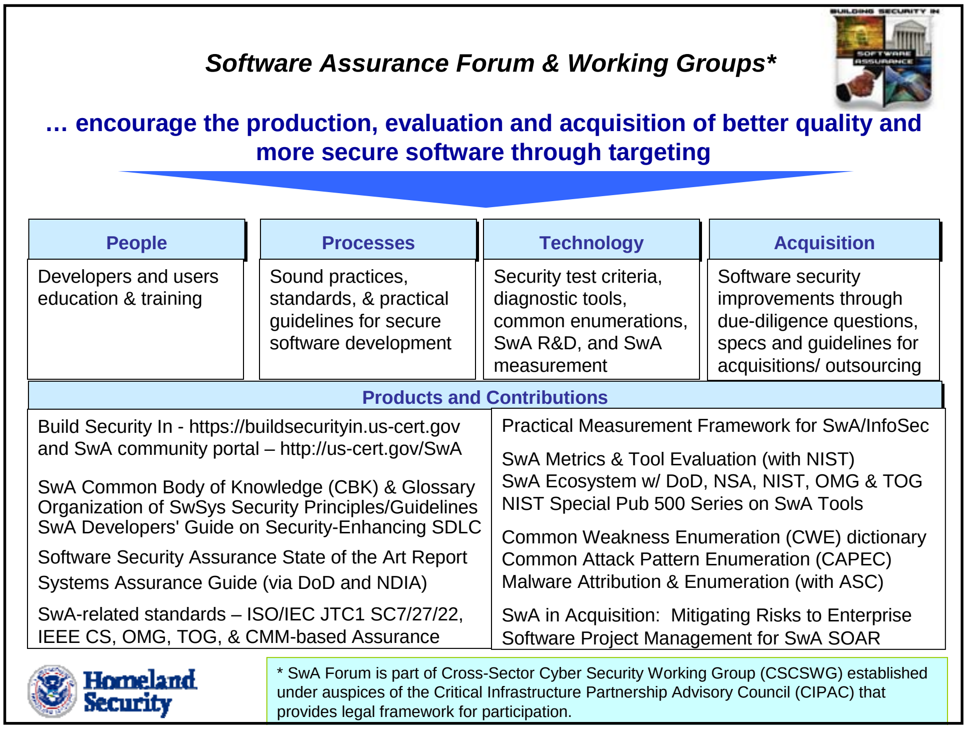
  "DHS will facilitate a national public-private effort to promulgate best practices and methodologies that promote integrity, security, and reliability in software code development, including processes and procedures that diminish the possibilities of erroneous code, malicious code, or trap doors that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

- DHS Program goals promote the security and resilience 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 and applicable standards and 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



*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

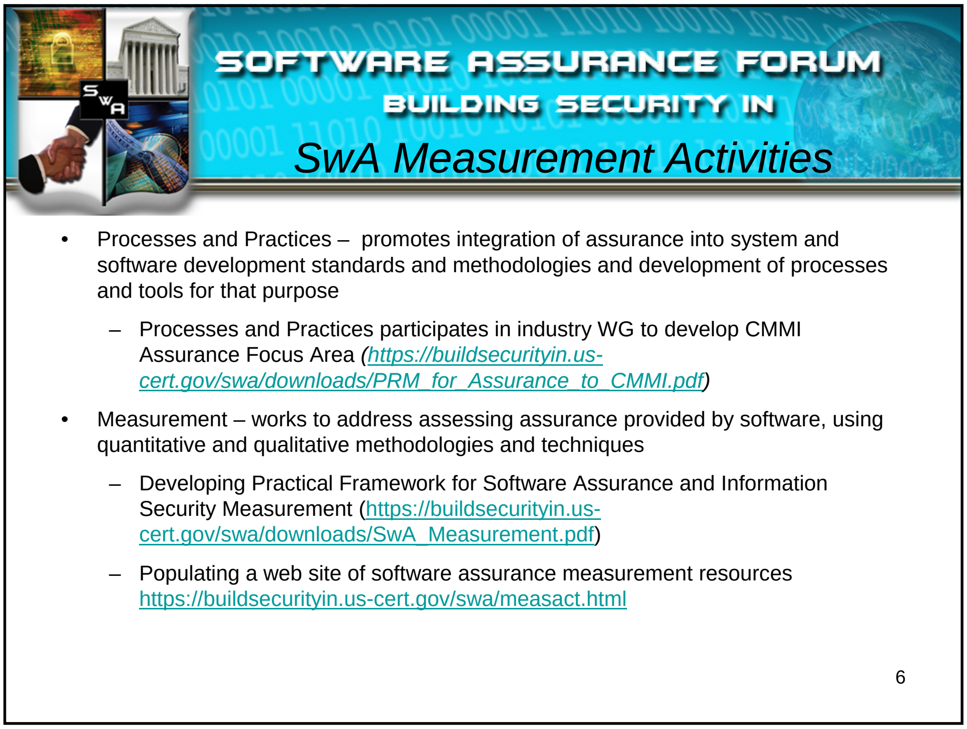
SwA Metrics & Tool Evaluation (with NIST)
SwA Ecosystem w/ DoD, NSA, NIST, OMG & TOG
NIST Special Pub 500 Series on SwA Tools

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

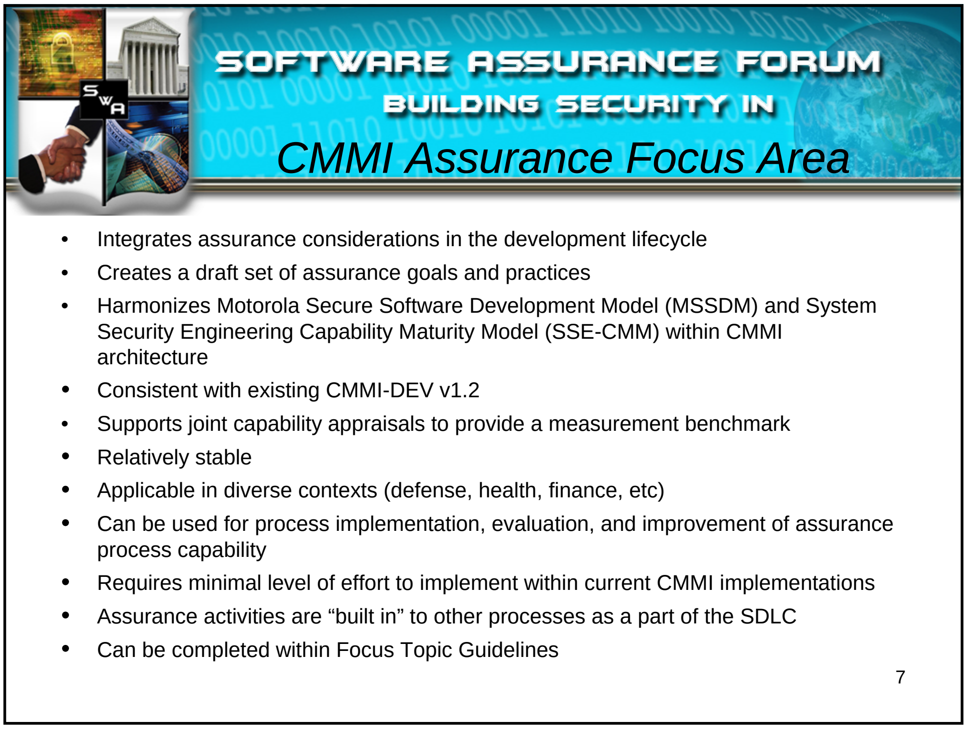
* SwA Forum is part of Cross-Sector Cyber Security Working Group (CSCSWG) established under auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC) that provides legal framework for participation.



SOFTWARE ASSURANCE FORUM
BUILDING SECURITY IN

SwA Measurement Activities

- Processes and Practices – 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*)
- Measurement – 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

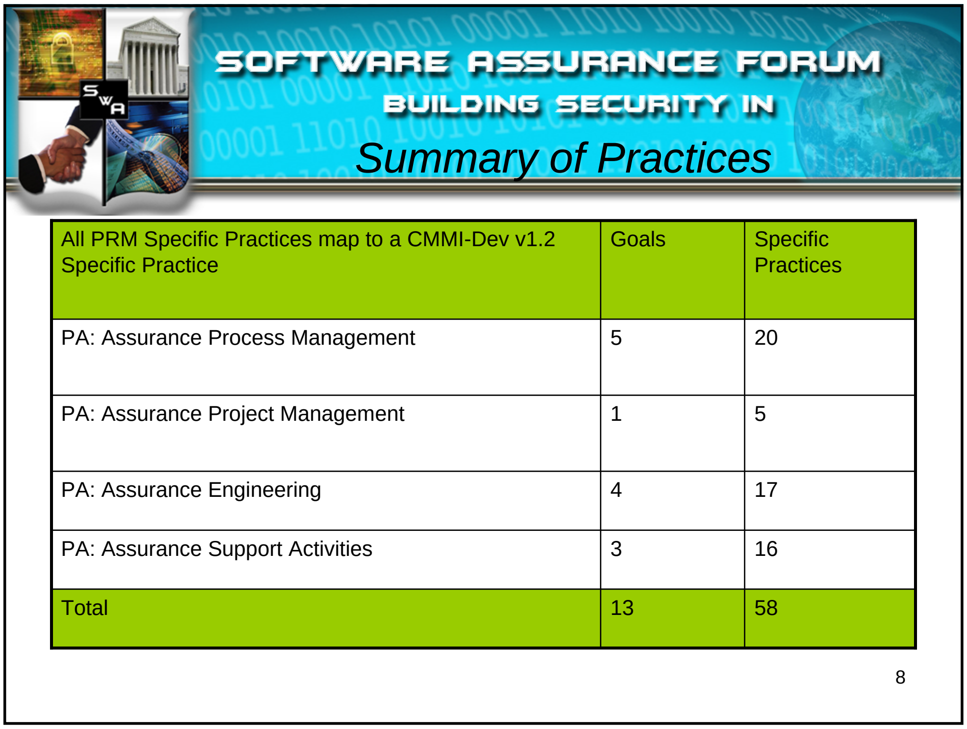


SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

CMMI Assurance Focus Area

- Integrates assurance considerations in the development lifecycle
- Creates a draft set of assurance goals and practices
- Harmonizes Motorola Secure Software Development Model (MSSDM) and System Security Engineering Capability Maturity Model (SSE-CMM) 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



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Summary of Practices

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

SOFTWARE ASSURANCE FORUM
BUILDING SECURITY IN

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

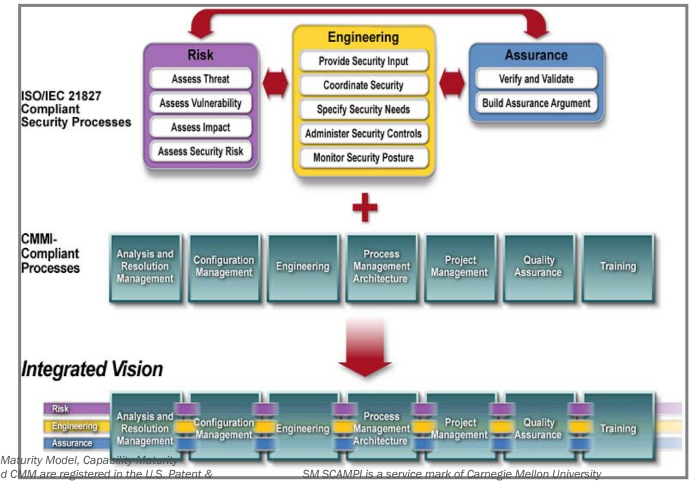
SOFTWARE ASSURANCE FORUM
BUILDING SECURITY IN

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.	Sub Practice 2.2.4.1 Define project assurance goals and measures.	MA Measurement and Analysis	SP 1.1 Establish measurement objective SP 1.2 Specify 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

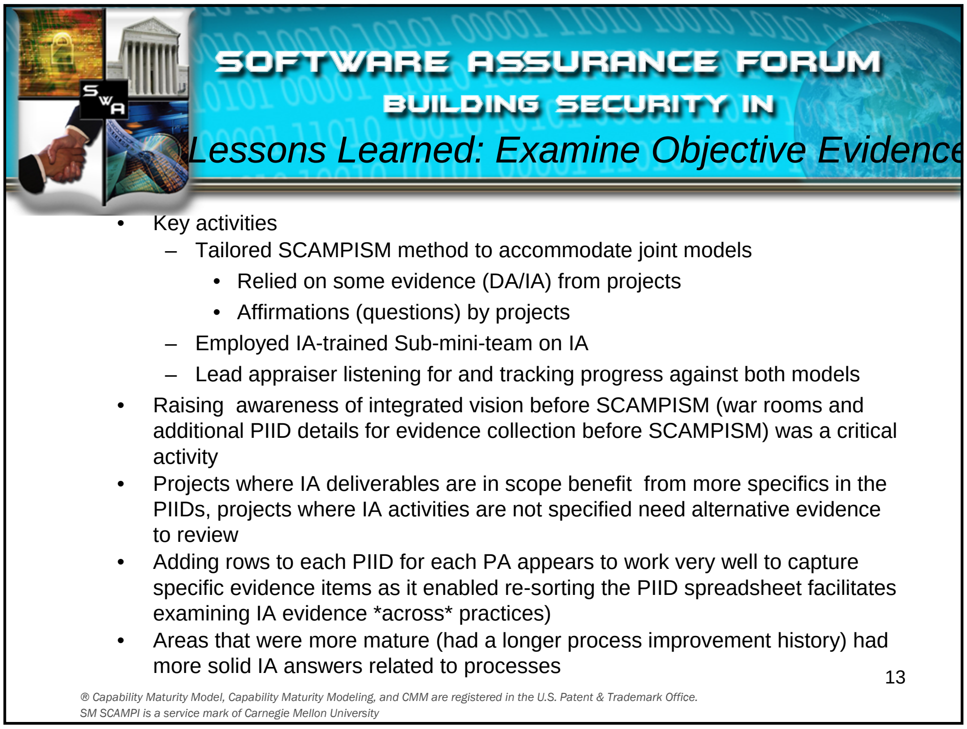
Color Legend	
Blue: PRM Process Area	**Purple:** PRM Informative material to assist with implementing practices
Yellow: PRM Goals	**Pink:** CMMI Process Areas
Green: PRM Practices that support a goal	**Orange:** CMMI Specific Practices that support a goal

Example Implementation



Lessons Learned: Prepare and Plan

- Key Activities
  - Sponsor initiated planning for an integrated appraisal led by an external lead appraiser
  - Tailoring and adjustments to the SCAMPISM method and objectives for the appraisal were made
  - September 2007 - Appraisal Objective leverage existing PIID data and interviews to characterize SSE-CMM with relevant CMMI ® PA and report to organization with appraisal results)
- There was no place in the PIID to capture most of the organizational management and IA-related evidence at the organizational level
- For SSE-CMM, an agreed-upon mapping between CMMI ®, SSE-CMM and OSP/PDPs must be completed for the appraisal team/PIID use
- Need some basic training for SSE-CMM (or whatever model is in play) for interpretation reasons – Team members have difficulty shifting between model paradigms
- Identify IA PIID elements *with suggestions and more guidance for projects* - helps projects identify evidence for IA practices ahead of the SCAMPISM, so there is less discovery

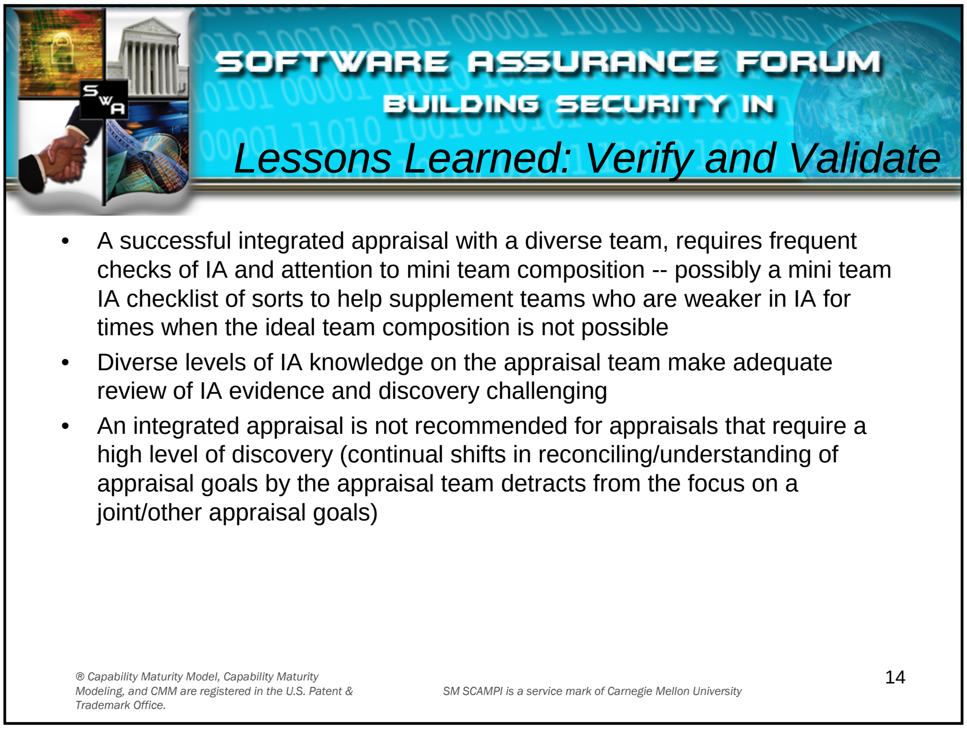


SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Lessons Learned: Examine Objective Evidenc

- Key activities
  - – Tailored SCAMPISM method to accommodate joint models
    - Relied on some evidence (DA/IA) from projects
    - Affirmations (questions) by projects
  - – Employed IA-trained Sub-mini-team on IA
  - – Lead appraiser listening for and tracking progress against both models
- Raising awareness of integrated vision before SCAMPISM (war rooms and additional PIID details for evidence collection before SCAMPISM) was a critical activity
- Projects where IA deliverables are in scope benefit from more specifics in the PIIDs, projects where IA activities are not specified need alternative evidence to review
- Adding rows to each PIID for each PA appears to work very well to capture specific evidence items as it enabled re-sorting the PIID spreadsheet facilitates examining IA evidence *across* practices)
- Areas that were more mature (had a longer process improvement history) had more solid IA answers related to processes

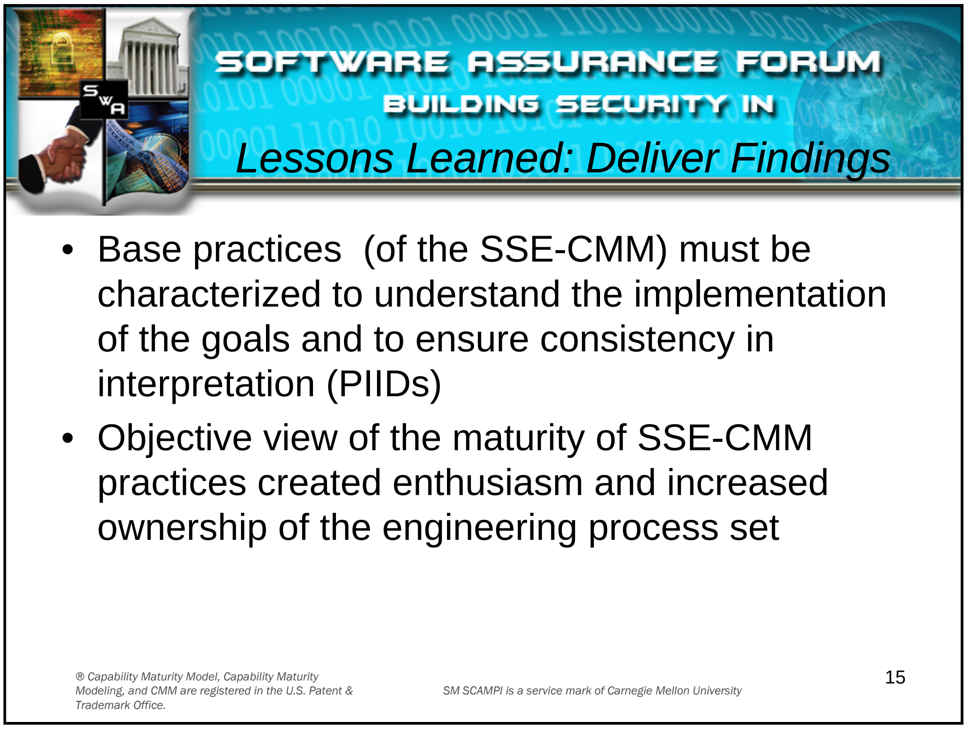


SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Lessons Learned: Verify and Validate

- A successful integrated appraisal with a diverse team, requires frequent checks of IA and attention to mini team composition -- possibly a mini team IA checklist of sorts to help supplement teams who are weaker in IA for times when the ideal team composition is not possible
- Diverse levels of IA knowledge on the appraisal team make adequate review of IA evidence and discovery challenging
- An integrated appraisal is not recommended for appraisals that require a high level of discovery (continual shifts in reconciling/understanding of appraisal goals by the appraisal team detracts from the focus on a joint/other appraisal goals)

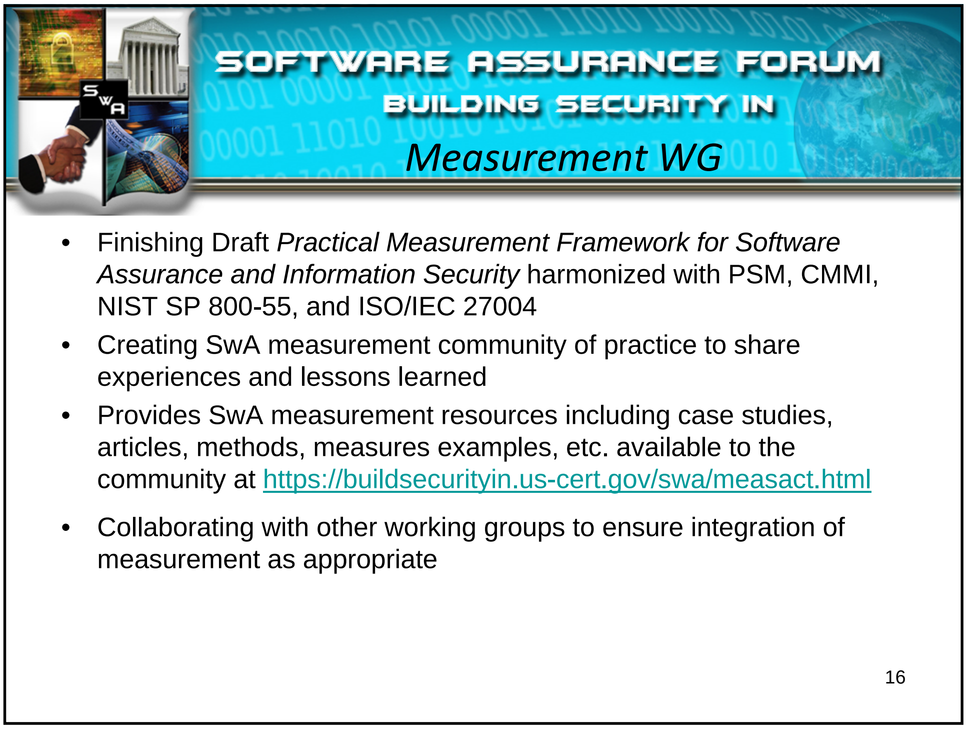


Lessons Learned: Deliver Findings

- Base practices (of the SSE-CMM) must be characterized to understand the implementation of the goals and to ensure consistency in interpretation (PIIDs)
- Objective view of the maturity of SSE-CMM practices created enthusiasm and increased ownership of the engineering process set

® Capability Maturity Model, Capability Maturity Modeling, and CMM are registered in the U.S. Patent & Trademark Office.

SM SCAMPI is a service mark of Carnegie Mellon University



Measurement WG

- Finishing Draft *Practical Measurement Framework for Software Assurance and Information Security* harmonized with PSM, CMMI, NIST SP 800-55, and ISO/IEC 27004
- Creating SwA measurement community of practice to share experiences and lessons learned
- Provides SwA measurement resources including case studies, articles, methods, measures examples, etc. available to the community at https://buildsecurityin.us-cert.gov/swa/measact.html
- Collaborating with other working groups to ensure integration of measurement as appropriate

Measurement Framework Summary

This document does

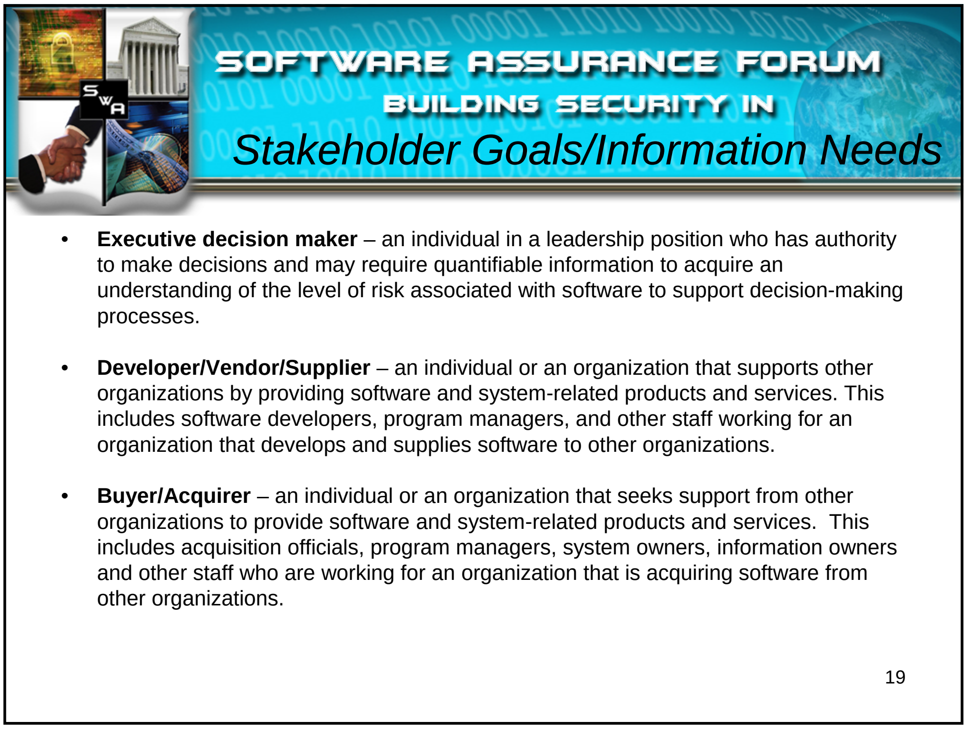
- Explain how to integrate SwA measurement into existing measurement approaches
- Provide a common framework for addressing SwA measurement regardless of what measurement approach is used
- Explain a basic process for measurement common to referenced measurement methodologies
- Provide example goals/information needs and measures for three primary SwA stakeholder groups
- Contain measures based on common enumerations to get to tangible software-related things to measure

This document does not

- Create a new stand-alone measurement approach for SwA
- Provide a single text book for SwA measurement that can be used without referencing other methods
- List ALL possible SwA measures that could be ever needed by a project or organization

SwA Measurement Principles

- SwA measurement is a composite discipline and can be implemented by including SwA goals and objectives in a project or organizational measures development and implementation regardless of what specific measurement methodology is being used.
- SwA measurement must satisfy information needs of a variety of stakeholders/audiences, including executives, developers, vendors, suppliers and buyers.
- Each stakeholder group will require tailoring of specific measures based on each group’s information needs.
- Different measures targeting different stakeholders may use the same information originating from the same data sources to facilitate multiple uses of the same set of data.
- SwA measures must be cost effective and practical to help focus resources on improving secure design and coding practices.
- Implementation of SwA measures should facilitate automation of data collection and reporting
- Each phase of the SDLC, acquisition life cycle, or any other life cycle introduces an opportunity to measure SwA and improve its results.
- For the purposes of this document, the term “measurement” applies to both quantitative and qualitative measurement methodologies.

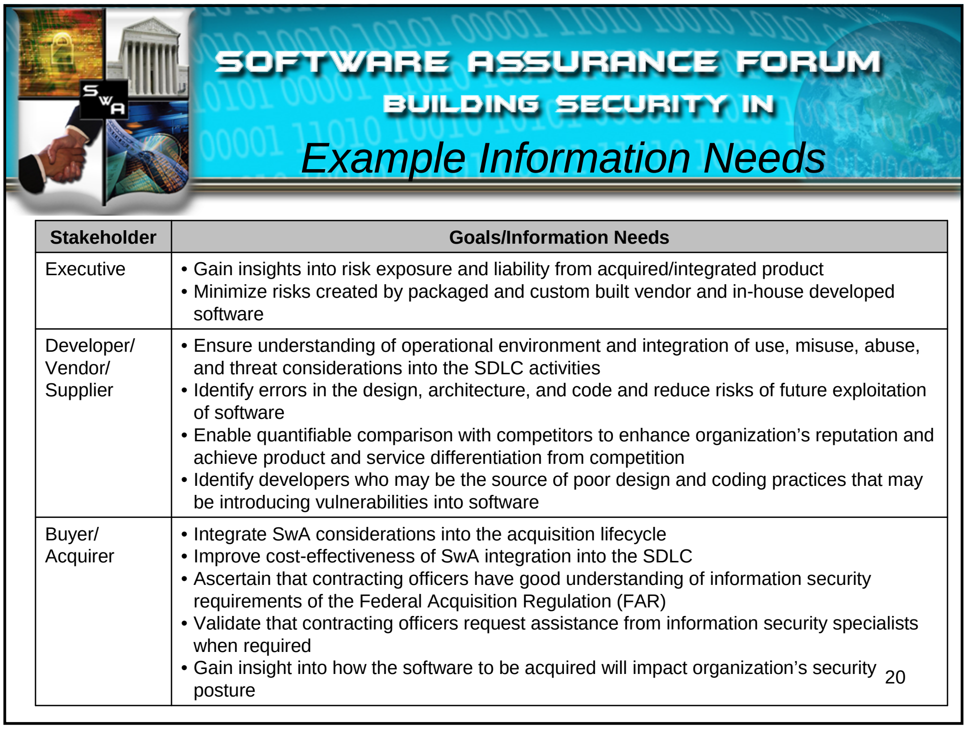


Stakeholder Goals/Information Needs

- **Executive decision maker** – an individual in a leadership position who has authority to make decisions and may require quantifiable information to acquire an understanding of the level of risk associated with software to support decision-making processes.

- **Developer/Vendor/Supplier** – an individual or an organization that supports other organizations by providing software and system-related products and services. This includes software developers, program managers, and other staff working for an organization that develops and supplies software to other organizations.

- **Buyer/Acquirer** – an individual or an organization that seeks support from other organizations to provide software and system-related products and services. This includes acquisition officials, program managers, system owners, information owners and other staff who are working for an organization that is acquiring software from other organizations.



Example Information Needs

Stakeholder	Goals/Information Needs
Executive	• Gain insights into risk exposure and liability from acquired/integrated product • Minimize risks created by packaged and custom built vendor and in-house developed software
Developer/ Vendor/ Supplier	• Ensure understanding of operational environment and integration of use, misuse, abuse, and threat considerations into the SDLC activities • Identify errors in the design, architecture, and code and reduce risks of future exploitation of software • Enable quantifiable comparison with competitors to enhance organization's reputation and achieve product and service differentiation from competition • Identify developers who may be the source of poor design and coding practices that may be introducing vulnerabilities into software
Buyer/ Acquirer	• Integrate SwA considerations into the acquisition lifecycle • Improve cost-effectiveness of SwA integration into the SDLC • Ascertain that contracting officers have good understanding of information security requirements of the Federal Acquisition Regulation (FAR) • Validate that contracting officers request assistance from information security specialists when required • Gain insight into how the software to be acquired will impact organization's security posture

SOFTWARE ASSURANCE FORUM

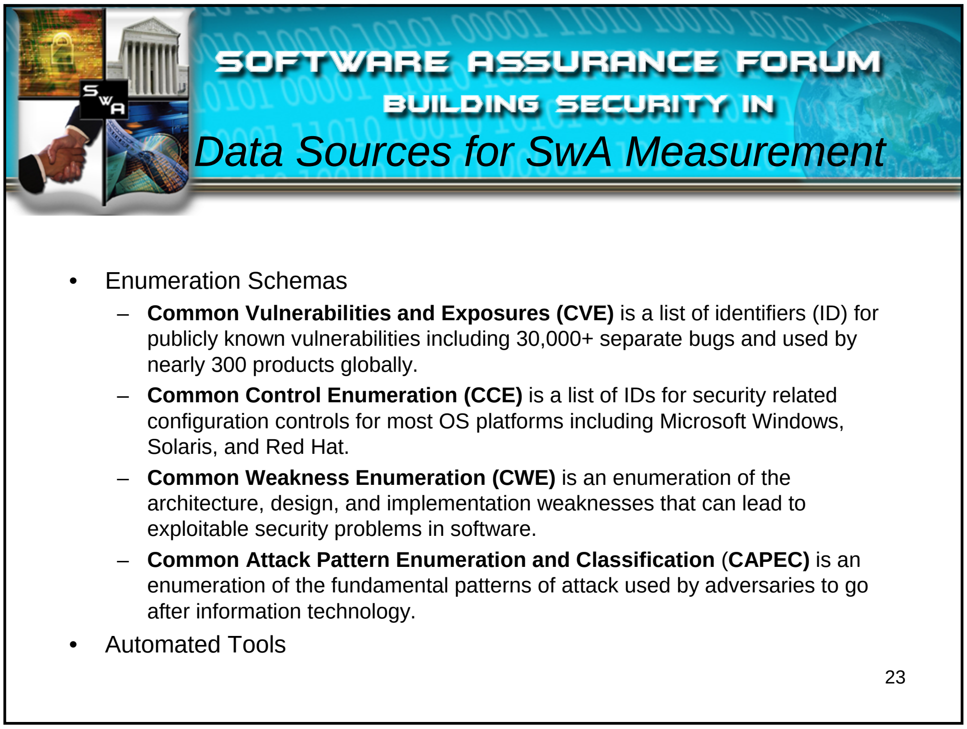
BUILDING SECURITY IN

Example Measures

Project Activity	Measures	Information Need	Benefit
Development	• Number of discovered defects that are known as software vulnerabilities (e.g. buffer overflows and cross-site scripting) • Number of user-controllable inputs • Number of deviations between design, code and requirements • Number of times high risk statements (e.g., commands, APIs) are used • Percent of code coverage for which appropriate exception handling has been created • Percent of discovered defects that were fixed	• Proactively address the security defects prior to testing and deployment • Assure that the application performs exception handling as required	• Minimizes development and maintenance rework costs • Reduces the chances of introducing vulnerabilities Increases predictability of software behavior

Measurement Framework Overview

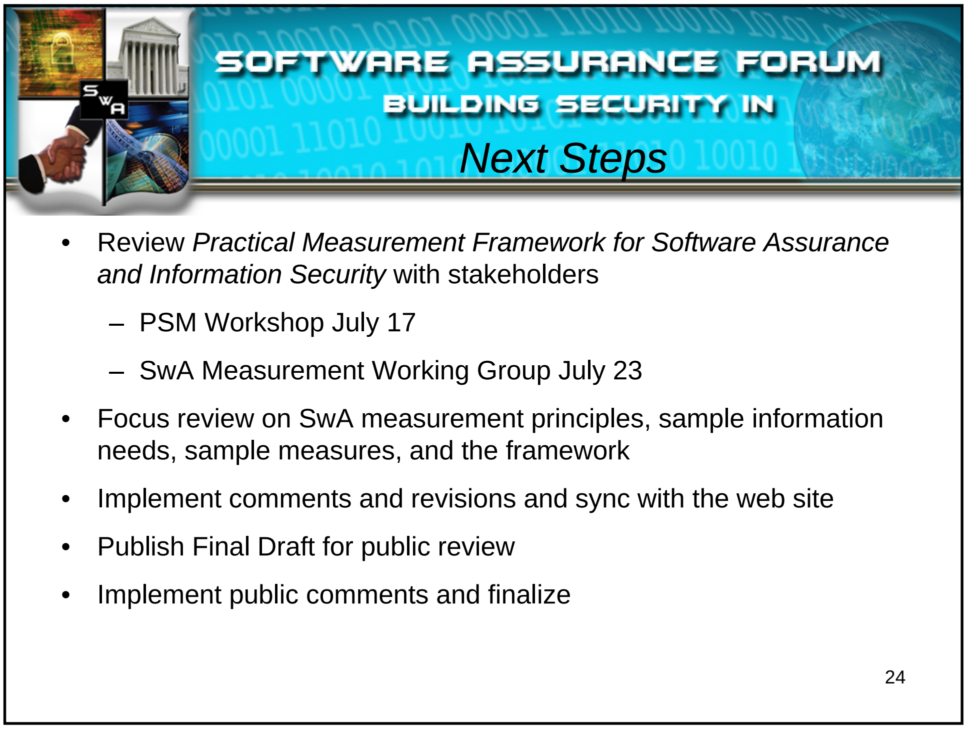
	Software & Systems			Information Security	
	PSM ISO/IEC 15939	CMMI® (Measurement and Analysis Process Area)	CMMI® GQ(I)M	ISO/IEC 27004	NIST SP 800-55 Revision 1
Goal/ Objective/ Information Need Description	Information Need	**SG 1: SP 1.1** Establish measurement objectives.	Objective	Purpose of measure	Goal and Objective
	Information Category			Control or Control Objective	
Measurable Concept/ Question	Measurable Concept		Question		
Entities/ Attributes	Relevant Entities		Data Elements	Object of Measurement	
	Attributes		Data Elements	Attributes	
Base Measure Specification	Base Measure		Data Elements	Base Measure	Measure
	Measurement Method		Data Collection - How	Measurement Method	
	Type of Method	Specify Measures	Data Collection - How		
	Scale	Specify Measures	Inputs - Definition	Scale	
	Type of Scale	Specify Measures	Inputs - Definition	Scale	
	Unit of Measurement	Specify Measures	Inputs - Definition:		
Derived Measure Specification	Derived Measure	Specify Measures; Collect Measurement Data	Inputs - Data Elements	Derived Measure	Measure
	Measurement Function	Specify Measures	Algorithm	Measurement Function	Formula
Indicator Specification	Indicator Description and Sample	Specify Measures; Analyze Measurement Data	Indicator/Visual Display	Indicator Description and Sample	
	Analysis Model	Specify Measures; Analyze Measurement Data	Analysis	Analytical Model	Implementation Evidence
	Decision Criteria	Specify Analysis Procedures		Decision Criteria	Implementation Evidence
	Indicator Interpretation	Analyze Measurement Data; Communicate Results	Interpretation	Indicator Interpretation; Effects/Impact; Causes of deviation; Positive values;	Target; Type; Reporting Format
Data Collection and Storage Procedures	Frequency of Data Collection	Specify Data Collection and Storage Procedures	Data Collection - When/How Often	Frequency of collection	Frequency
	Responsible Individual	Specify Data Collection and Storage Procedures	Data Collection - By Whom	Information Collector	Responsible Parties
	Phase or Activity in which Collected	Specify Data Collection and Storage Procedures	Data Collection - When/How Often	Measure valid up to; Period of Analysis	
	Tools Used in Data Collection	Specify Data Collection and Storage Procedures	Data Collection - Forms	Tools Used in Data Collection	Data Source
	Verification and Validation:	Collect Measurement Data	Data Storage - How	Collection Date; Reviewer; Information	
	Repository for Collected Data	Specify Data Collection and Storage Procedures	Data Storage - Where; How, Security	Repository for Collected Data	
Analysis and Reporting Procedures	Frequency of Data Reporting	Specify Analysis Procedures	Data Reporting - How Often	Frequency of Data Reporting	Frequency
	Responsible Individual	Specify Analysis Procedures	Data Reporting - Responsibility of	Information Communicato	Responsible Parties
	Phase or Activity in which Analyzed	Specify Analysis Procedures	Assumptions	Measure valid up to; Period of Analysis	
	Source of Data for Analysis	Specify Analysis Procedures	Data Elements	Source of Data for Analysis	Data Source
	Tools Used in Analysis	Specify Analysis Procedures	Data Collection -	Tools Used in Analysis	
	Review, Report, or User	Store Data and Results; Communicate Results	Data Reporting - By/To Whom; Perspective	Information Client; Reviewer	Responsible Parties
Additional Information	Additional Analysis Guidance	Analyze Measurement Data	Evolution	Additional Analysis Guidance	
	Implementation Considerations	Analyze Measurement Data	X-references	Implementation Considerations	



SOFTWARE ASSURANCE FORUM
BUILDING SECURITY IN

Data Sources for SwA Measurement

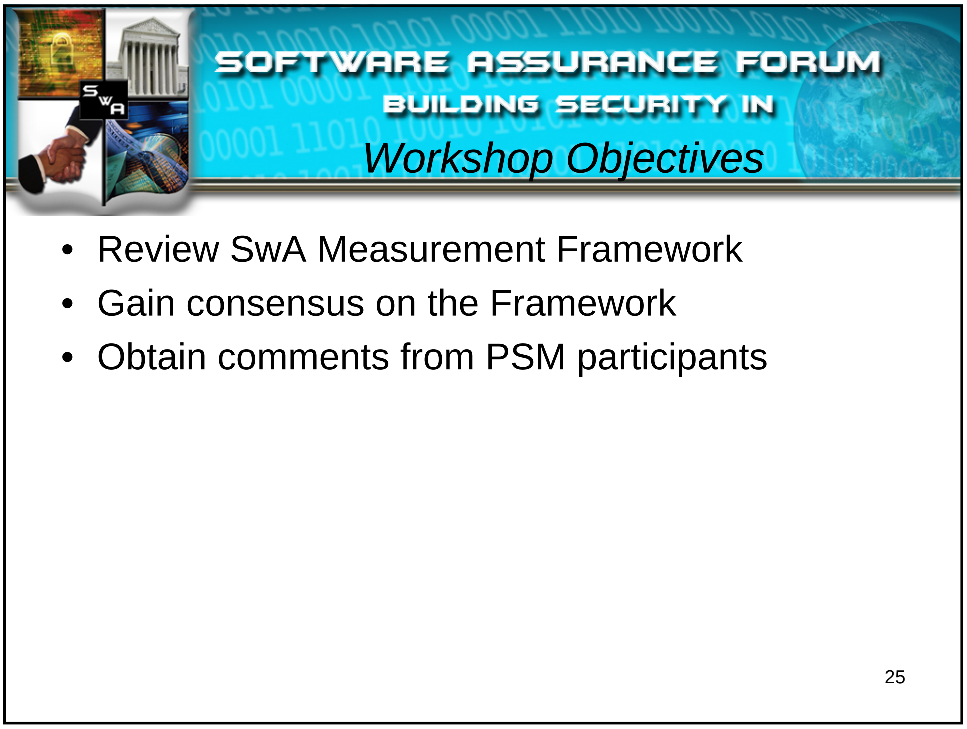
- Enumeration Schemas
  - **Common Vulnerabilities and Exposures (CVE)** is a list of identifiers (ID) for publicly known vulnerabilities including 30,000+ separate bugs and used by nearly 300 products globally.
  - **Common Control Enumeration (CCE)** is a list of IDs for security related configuration controls for most OS platforms including Microsoft Windows, Solaris, and Red Hat.
  - **Common Weakness Enumeration (CWE)** is an enumeration of the architecture, design, and implementation weaknesses that can lead to exploitable security problems in software.
  - **Common Attack Pattern Enumeration and Classification** (**CAPEC)** is an enumeration of the fundamental patterns of attack used by adversaries to go after information technology.
- Automated Tools



SOFTWARE ASSURANCE FORUM
BUILDING SECURITY IN

Next Steps

- Review *Practical Measurement Framework for Software Assurance and Information Security* with stakeholders
  - PSM Workshop July 17
  - SwA Measurement Working Group July 23
- Focus review on SwA measurement principles, sample information needs, sample measures, and the framework
- Implement comments and revisions and sync with the web site
- Publish Final Draft for public review
- Implement public comments and finalize

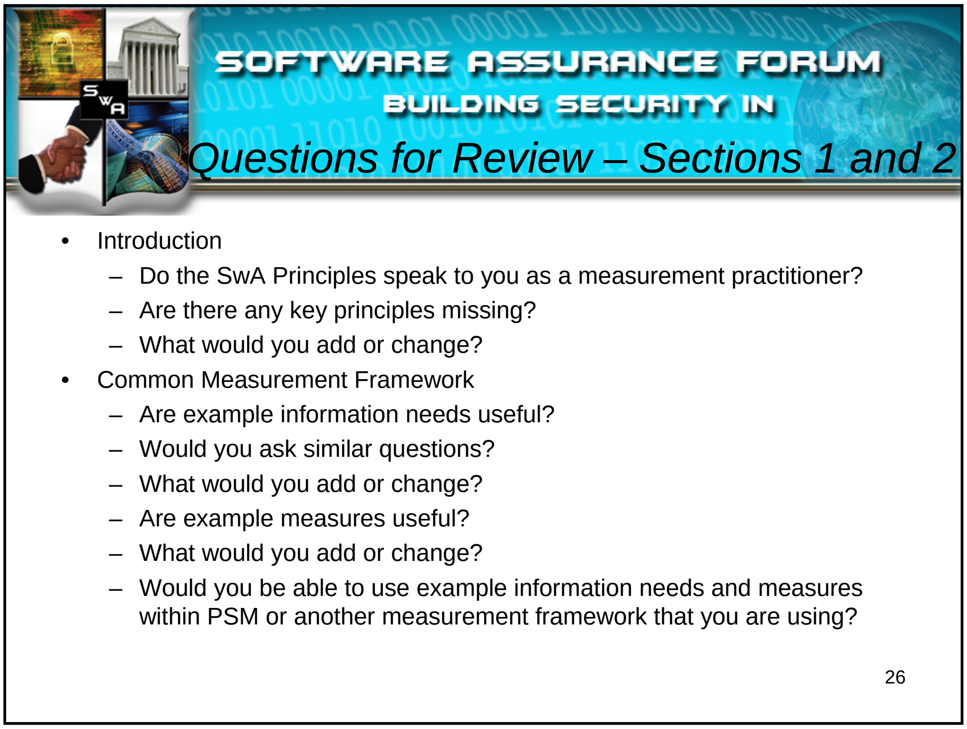


SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Workshop Objectives

- Review SwA Measurement Framework
- Gain consensus on the Framework
- Obtain comments from PSM participants

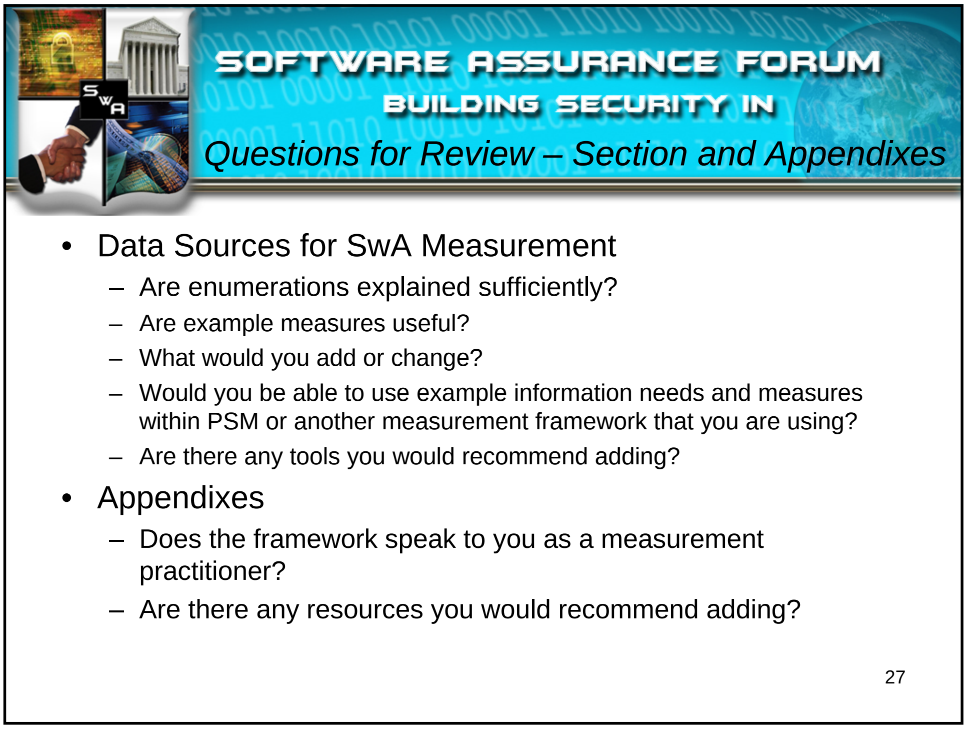


SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Questions for Review – Sections 1 and 2

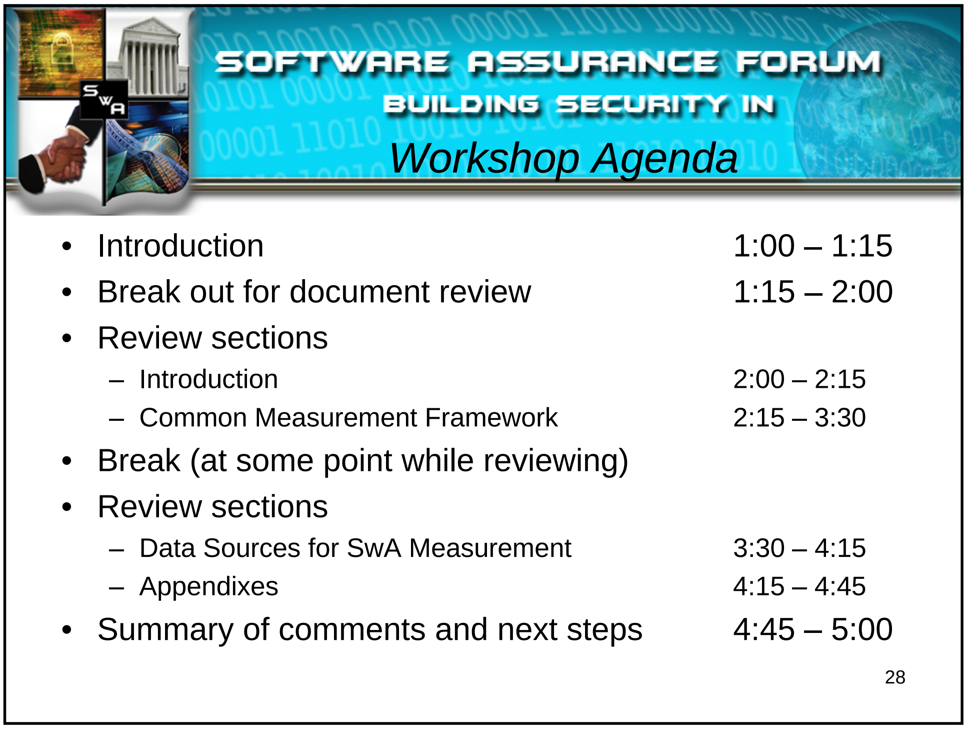
- Introduction
  - Do the SwA Principles speak to you as a measurement practitioner?
  - Are there any key principles missing?
  - What would you add or change?
- Common Measurement Framework
  - Are example information needs useful?
  - Would you ask similar questions?
  - What would you add or change?
  - Are example measures useful?
  - What would you add or change?
  - Would you be able to use example information needs and measures within PSM or another measurement framework that you are using?



SOFTWARE ASSURANCE FORUM
BUILDING SECURITY IN

Questions for Review – Section and Appendixes

- Data Sources for SwA Measurement
  - Are enumerations explained sufficiently?
  - Are example measures useful?
  - What would you add or change?
  - Would you be able to use example information needs and measures within PSM or another measurement framework that you are using?
  - Are there any tools you would recommend adding?
- Appendixes
  - Does the framework speak to you as a measurement practitioner?
  - Are there any resources you would recommend adding?



SOFTWARE ASSURANCE FORUM
BUILDING SECURITY IN

Workshop Agenda

• Introduction	1:00 – 1:15
• Break out for document review	1:15 – 2:00
• Review sections	
– Introduction	2:00 – 2:15
– Common Measurement Framework	2:15 – 3:30
• Break (at some point while reviewing)	
• Review sections	
– Data Sources for SwA Measurement	3:30 – 4:15
– Appendixes	4:15 – 4:45
• Summary of comments and next steps	4:45 – 5:00

Contact Info

- Joe Jarzombek, PMP
  Director for Software Assurance, National Cyber Security Division
  Office of Assistant Secretary for Cyber Security & Communications
  Department of Homeland Security
  Joe.Jarzombek@dhs.gov
  http://www.us-cert.gov/swa/
  https://**buildsecurityin**.us-cert.gov

- Nadya Bartol, CISSP, ISSPCS, SSE CMM Lead Appraiser
  Co-Chair DHS SwA Measurement Working Group
  bartol_nadya@bah.com