Leveraging Models And Standards For Assurance

Paul R. Croll
CSC
pcroll@csc.com

Michele Moss
Booz Allen Hamilton
moss_michele@bah.com

Co-Chairs, DHS Software Assurance Forum Working Group on Processes and Practices

Topics

- What Is System and Software Assurance?
- The Assurance Problem
- Leveraging Models And Standards For Assurance
- Summary

What Is System and Software Assurance?

- 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.

  CNSS Instruction No. 4009, "National Information Assurance Glossary," Revised 2006

- Grounds for confidence that an entity meets its relevant needs, goals or objectives for safety, security and dependability or other characteristics deemed to be critical, and possesses the related required properties.

  ISO/IEC CD 15026, 2007, Systems and Software Assurance

The Assurance Problem

- Assurance-related risks have dramatically increased due to the simultaneous growth in software vulnerabilities and in threat opportunities
- Risk management processes inadequately address these threats and risks
- Threats presented by suppliers of software products and services are not adequately identified and analyzed
- Development and acquisition processes inadequately address assurance
- There is a fundamental lack of both the scientific understanding of software risks, and the capabilities to effectively diagnose and mitigate them in the in a timely manner

Source: J. Jarzombek. DOD Software Assurance Initiative: Mitigating Risks Attributable to Software. DOD Software Assurance Forum, July 2004.

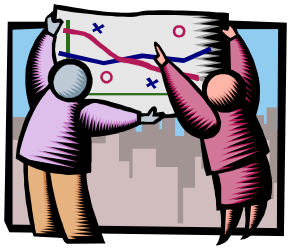
The Solution Requires A Balance Of Benchmarks

- A Security example:
  - The chicken….
    - Process Capability Assessment (CMMI ® Capability Maturity Model Integration, iCMM FAA Integrated Capability Maturity Model and Safety and Security extensions, ISO/IEC 21827 System Security Engineering Capability Maturity Model (SSE CMM))
    - Management Systems (ISO/IEC 27001 Information Security Management System (ISMS), ISO 9001 – Quality Management)
  - The egg …
    - IA Controls (NIST SP 800-53, DOD 8500.02) and C&A Methodologies (NIST SP 800-37, DIACAP)
    - Common Criteria, ISO 15408, Information Technology - Security Techniques - Evaluation criteria for IT security
    - Static Code Analysis

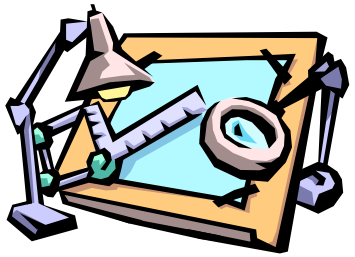
Leveraging Models And Standards For Assurance

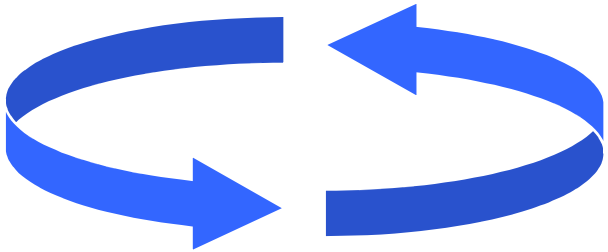
Measure Your Results

Understand Your Business Requirements for Assurance



Build or Refine and Execute Your Assurance Processes





Understand Assurance-Related Process Capability Expectations

Look to Standards for Assurance Process Detail

Understand Your Business Requirements for Assurance

- Legal and regulatory requirements
- Product/Service-specific requirements
- Customer-specific requirements
- Business process requirements

Understand Assurance-Related Process Capability Expectations

- The CMMI®- DEV does not treat assurance adequately
  - Inconsistent treatment of safety and security concerns
  - Insufficient assurance detail in required and expected components
    - Specific goals
    - Specific practices
  - Insufficient traceability to assurance source standards

CMMI® – DEV Process Areas and Assurance

Name	*Abbr*	*Safety*	*Security*
Requirements Management	REQM	√	√
Project Planning	PP	√	√
Project Monitoring and Control	PMC		√
Supplier Agreement Management	SAM		√
Measurement and Analysis	MA		√
Process and Product Quality Assurance	PPQA		
Configuration Management	CM	√	√
Requirements Development	RD	√	√
Technical Solution	TS	√	√
Product Integration	PI	√	√
Verification	VER		
Validation	VAL		
Organizational Process Focus	OPF		
Organizational Process Definition +IPPD	OPD +IPPD	√	√
Organizational Training	OT	√	√
Integrated Project Management +IPPD	IPM +IPPD	√	√
Risk Management	RSKM	√	√
Decision Analysis and Resolution	DAR	√	
Organizational Process Performance	OPP		
Quantitative Project Management	QPM		
Organizational Innovation and Deployment	OID		
Causal Analysis and Resolution	CAR	√	

Source: CMMI® for Development, Version 1.2, CMU/SEI-2006-TR-008, August 2006

Improving Process Capability Expectations For Assurance

- Current industry effort underway to
  - Harmonize existing Security Capability Maturity Models (MSSDM, SSE-CMM) expertise and experience
  - Present the results in a way that is easy for CMMI users to implement
- Success Criteria
  - Define process capability for assurance at a level of detail that is stable and in a way that is applicable in diverse contexts (Defense, National Security, Finance, Heath care, Aviation, Telecommunications)
  - Implementation (process implementation, assessment, and improvement) of assurance process capability requires minimal LOE to implement within current CMMI – implementations
  - Assurance activities are “built in” to other processes as a part of mission success
- The next slides contain draft material currently being refined and vetted by an industry effort for Assurance in the CMMI

Process Reference Model for Assurance: Process Areas and Goals – 1

PA1 - Assurance Process Management

SG1.1 Determine the assurance improvement opportunities to achieve key business goals.

- Identify and prioritize key business goals for assurance.

SG1.2 Establish the infrastructure to sustain the assurance program within the organization.

- Establish and maintain organizational assurance assets.

SG1.3 Establish and maintain an assurance culture for requirements, analysis, architecture, development, integration, and test.

- Establish a leadership advisory board for assurance.

Process Reference Model for Assurance: Process Areas and Goals – 2

PA2 - Assurance Project Management

SG2.1 Manage assurance activities against plans. All assurance aspects of the technical effort are planned.

- Plan and manage for assurance.

SG2.2 Establish and maintain an assurance infrastructure for the project.

- Communicate and coordinate all assurance decisions and recommendations.

SG2.3 Select, manage, and use effective suppliers and third party applications based upon their assurance capabilities.

- Understand the assurance risks related to the supplier.

Process Reference Model for Assurance: Process Areas and Goals – 3

PA3 - Assurance Engineering

SG3.1 Establish assurance requirements.

- o Understand the operating environment …

SG3.2 Architect a solution for assurance.

- o Architect and Design for assurance.

SG3.3 Implement a solution for assurance.

- o Implement a product design for assurance.

SG3.4 Verify and Validate the product assurance.

- o Verify and Validate an implementation for assurance.

SG3.5 Identify and manage risks throughout the product and system lifecycle.

- o Identify, characterize, and prioritize vulnerabilities and breaches.

Process Reference Model for Assurance: Process Areas and Goals – 4

PA4 - Assurance Support Management

SG4.1 Provide clear evidence that the work products meet the customer's assurance needs.

- Manage the assurance risk associated with operating the system within a defined environment.

SG4.2 Protect project and organizational assets.

- Detect and track both internal and external assurance related events.

Look to Standards for Assurance Process Detail – Programming Languages

- ISO/IEC SC22 – *OWG: Vulnerabilities* (OWGV)
  - **Project 22.24772**: Guidance for Avoiding Vulnerabilities through Language Selection and Use
    - Comparative guidance spanning multiple programming languages
    - Goal: Avoidance of programming errors that lead to vulnerabilities

Look to Standards for Assurance Process Detail – IT Security Techniques

- **ISO/IEC 15408**, Common Criteria for IT Security Evaluation
- **ISO/IEC 15443**, FRITSA
  - Part 1: A framework for IT security assurance
  - Part 2: Assurance methods
  - Part 3: Analysis of assurance methods
- **ISO/IEC 21827**, System Security Engineering Capability Maturity Model (SSE CMM) revision
- **ISO/IEC 27000** series – Information Security Management System (ISMS)

Look to Standards for Assurance Process Detail – Functional Safety

- IEC SC 65A
  - **IEC 61508**, Functional Safety Of Electrical/ Electronic/Programmable Electronic Safety-related Systems (7 parts)
    - Part 1: General requirements
    - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
    - Part 3: Software requirements
    - Part 4: Definitions and abbreviations
    - Part 5: Examples of methods for the determination of safety integrity levels
    - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
    - Part 7: Overview of techniques and measures
  - Risk-based approach for determining the required performance of safety-related systems

Look to Standards for Assurance Process Detail – Dependability

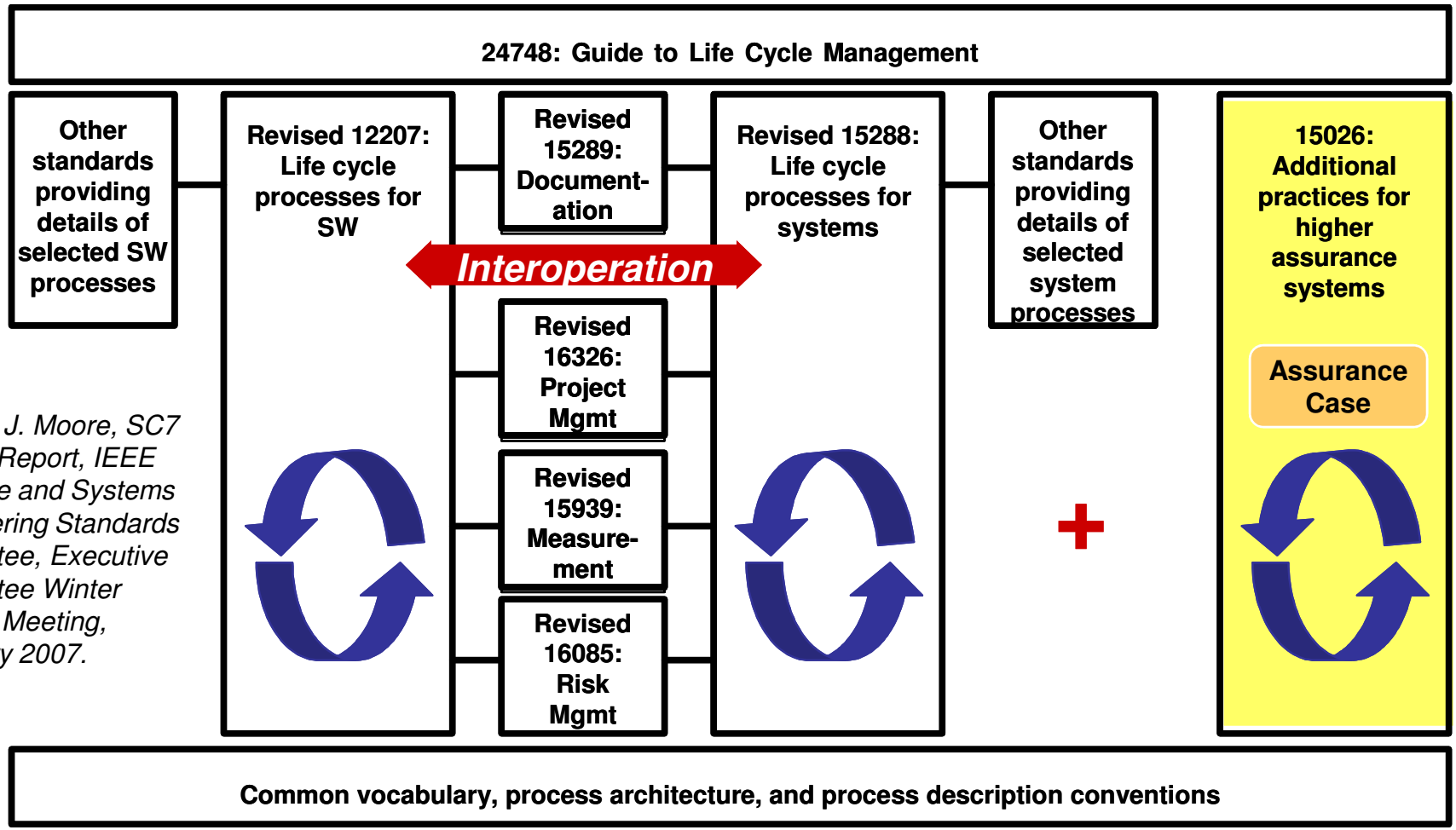
- **IEC 60300** Series, Dependability Management
- **IEC 61713**, Software dependability through the software life-cycle processes-Application guide
- **IEC 60812**, Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)
- **IEC 61025**, Fault tree analysis (FTA)

Look to Standards for Assurance Process Detail – FISMA[1] Implementation

- **FIPS Publication 199**, Standards for Security Categorization of Federal Information and Information System
- **FIPS Publication 200**, Minimum Security Requirements for Federal Information and Federal Information Systems
- **NIST Special Publication 800-30, Revision 1**, Risk Assessment Guideline
- **NIST Special Publication 800-37**, Guide for the Security Certification and Accreditation of Federal Information Systems
- **NIST Special Publication 800-39**, NIST Risk Management Framework
- **NIST Special Publication 800-53 Revision 2**, Recommended Security Controls for Federal Information Systems
- **NIST Special Publication 800-53A**, Guide for Assessing the Security Controls in Federal Information Systems
- **NIST Special Publication 800-59**, Guide for Identifying an Information System as a National Security System
- **NIST Special Publication 800-60**, Guide for Mapping Types of Information and Information Systems to Security Categories

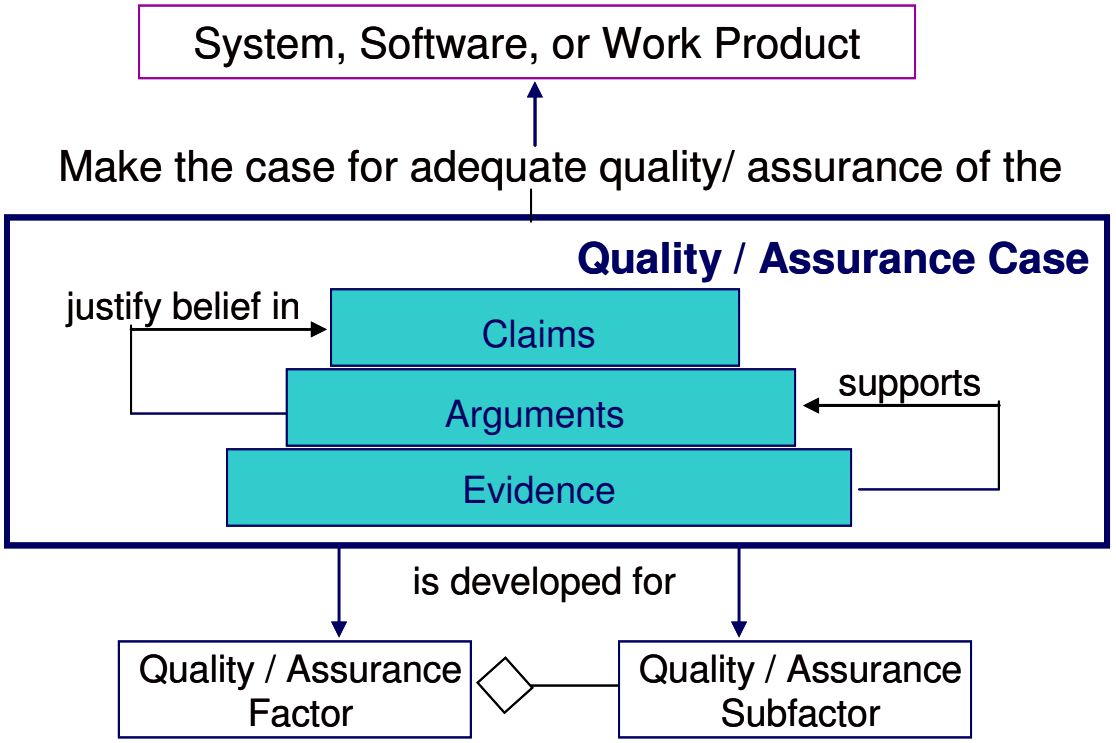
[1] *Federal Information Security Management Act of 2002*
*Source: **http://csrc.nist.gov/sec-cert/ca-proj-phases.html***

Look to Standards for Assurance Process Detail – Life Cycle Processes



Source: J. Moore, SC7 Liaison Report, IEEE Software and Systems Engineering Standards Committee, Executive Committee Winter Plenary Meeting, February 2007.

The Assurance Case In Relation To The Product And Its Quality/Assurance Factors



Attributes

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

Adapted from a slide by Joe Jarzombek who, in turn, credited IEEE CS alternative proposal for 15026 and CMU SEI QUASAR tutorial by Donald Firesmith, March 2007

Structure Of The Assurance Case

- Set of structured assurance claims, supported by evidence and reasoning, that demonstrates how assurance needs have been satisfied.
  - Shows compliance with assurance objectives
  - Provides an argument for the safety and security of the product or service.
  - Built, collected, and maintained throughout the life cycle
  - Derived from multiple sources
- Sub-parts
  - A high level summary
  - Justification that product or service is acceptably safe, secure, or dependable
  - Rationale for claiming a specified level of safety and security
  - Conformance with relevant standards and regulatory requirements
  - The configuration baseline
  - Identified hazards and threats and residual risk of each hazard and threat
  - Operational and support assumptions

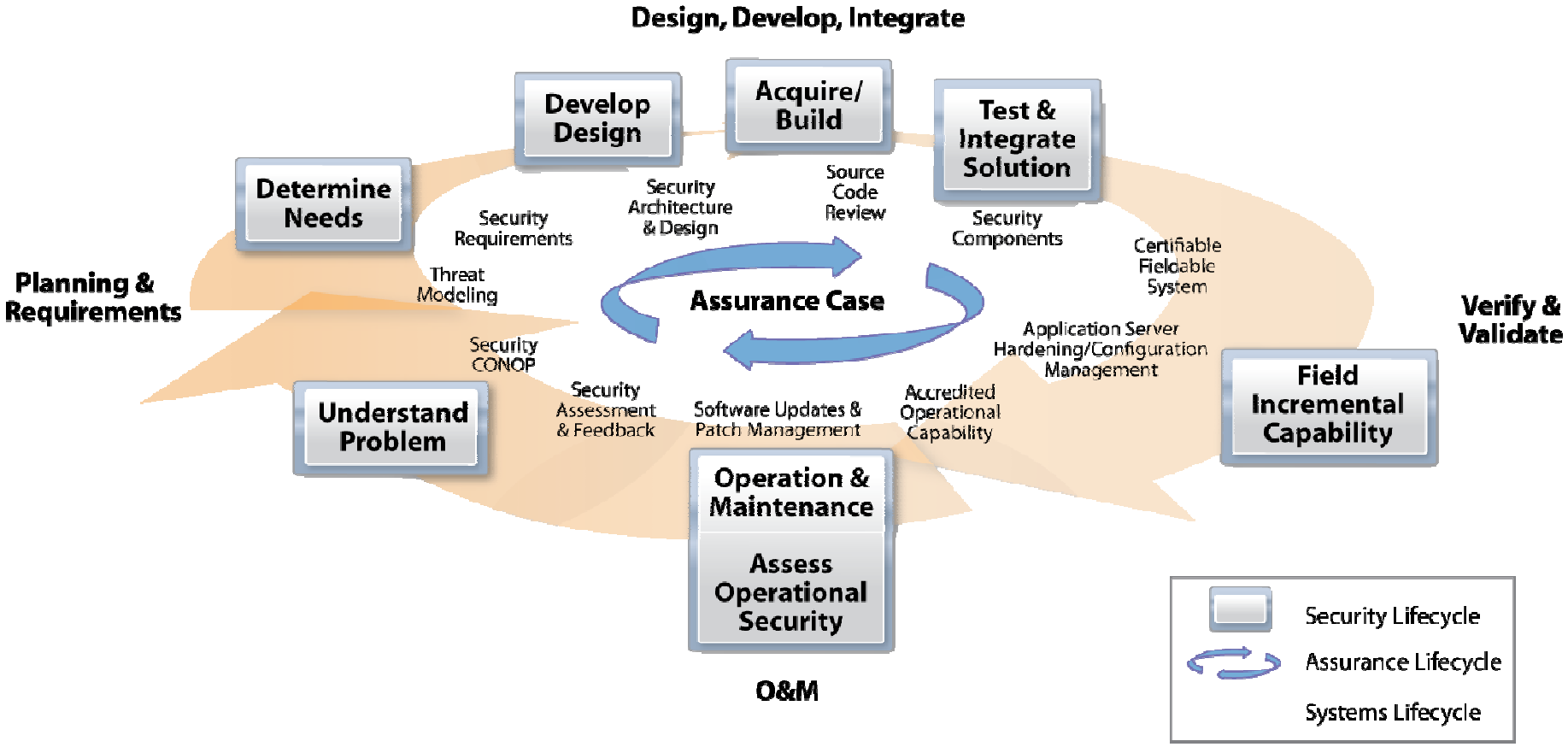
Additional Guidance on Assurance Processes – 1

- Systems Assurance – Delivering Mission Success in the Face of Developing Threats
  - An NDIA guidebook intended to supplement the knowledge of systems (and software) engineers who have responsibility for systems for which there are assurance concerns
- Security in the Software Life Cycle: Making Software Development Processes – and the Software Produced by Them – More Secure
  - An DHS report providing a compendium of methodologies, life cycle process models, sound practices, and supporting technologies that would, if adhered to, increase software security
- Software Assurance in Acquisition: Mitigating Risks to the Enterprise
  - A DHS report intended to provide guidance on enhancing supply chain management through improved risk mitigation and contracting for secure software
- State of the Art Report on Software Security Assurance
  - An IATAC/DACS report identifying and describing the current state of the art in software security assurance

Additional Guidance on Assurance Processes – 2

- Secure Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software
  - A DHS guidebook intended as a framework to identify workforce needs for competencies and leverage standards and best practices to guide software-related curriculum development
- ISO/IEC Technical Report – Guidance for Avoiding Vulnerabilities through Language Selection and Use

Build or Refine and Execute Your Assurance Processes



Measure Your Results - Modify Processes as Necessary

- Project Management
  - Schedule and Progress
  - Product Size and Stability
  - Customer Satisfaction
  - Resources and Cost
  - Product Quality (including assurance attributes)
  - Technical Effectiveness
  - Process Performance
- Compliance
  - FISMA
  - HIPPA
  - SOX
- Assurance
  - People (experience and training)
  - Process
  - Technology (Systems and Software)
  - Environment
- ROI
  - Cost avoidance
  - Risk Reduction
  - Business Enabler
- Process Management
  - CMMI
  - SSE-CMM

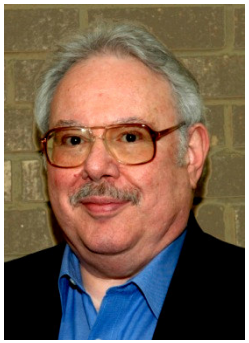
Summary

- Joint industry and Government efforts are ongoing to understand the strengths and weaknesses of current engineering practices and to provide appropriate guidance
- National and international standards efforts are also capturing and codifying minimum acceptable practice regarding engineering for systems assurance
- Additional Information Resources
  - https://buildsecurityin.us-cert.gov
  - http://iac.dtic.mil/iatac/
  - http://www.nist.gov
  - http://www.sei.cmu.edu/programs/nss/nss.html

For More Information . . .

Paul R. Croll
CSC
5166 Potomac Drive
King George, VA 22485-5824

Phone: +1 540.644.6224
Fax: +1 540.663.0276
e-mail: pcroll@csc.com



Michele Moss
Booz Allen Hamilton
8283 Greensboro Drive
McLean, VA 22102

Phone: +1 703.377.1254
Fax: +1 703.902.3595
e-mail: moss_michele@bah.com

References

G. Draper (ed.), *Top Software Engineering Issues Within Department of Defense and Defense Industry*. National Defense Industrial Association, Arlington, VA, August 2006.

K. Goertzel (ed.), *State of the Art Report on Software Security Assurance, Draft*. DOD Information Assurance Technical Assistance Center (IATAC) and the DOD Data and Analysis Center for Software (DACS), March 2007.

K. Goertzel (ed.), *Security in the Software Life Cycle: Making Software Development Processes – and the Software Produced by Them – More Secure, Draft 1.1*. U.S. Department of Homeland Security, July 2006.

J. Jarzombek. *DOD Software Assurance Initiative: Mitigating Risks Attributable to Software*. DOD Software Assurance Forum, July 2004.

National Defense Industrial Association Systems Assurance Guidebook. Version .89. National Defense Industrial Association, Arlington, VA, February, 2008.

S. Redwine (ed.), Secure *Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software, Draft 1.1*. U.S. Department of Homeland Security, September 25 2006.

Software Assurance in Acquisition: Mitigating Risks to the Enterprise, Draft 1.0. U.S. Department of Homeland Security, March 2007.

M. Nadworny, M. Moss, D. Beard, SEPG 2008 Software Capability Model for Assurance 20 March 2008