Practical Software Assurance and Security Measurement

Nadya Bartol
Joe Jarzombek

Homeland Security

Workshop Agenda

- Document 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

SOFTWARE ASSURANCE FORUM
BUILDING SECURITY IN

Introduction

- Background
- Purpose and Scope
- Assumptions
- Key Definitions
- Principles
- Document Structure

SOFTWARE ASSURANCE FORUM
BUILDING SECURITY IN

Common Measurement Framework

- Stakeholder Goals and Information Needs
- Key Measures
- Integrated Measurement Approach
  - Common Measure Specification
  - Implementing Measures

SOFTWARE ASSURANCE FORUM
BUILDING SECURITY IN

Data Sources for SwA Measurement

- Enumeration Schemas
- Automated Tools

SOFTWARE ASSURANCE FORUM
BUILDING SECURITY IN

Appendixes

- Appendix A – References
- Appendix B – Acronyms
- Appendix C – Definitions
- Appendix D – Measurement Methodologies and Resources
- Appendix E – Common Measure Specification

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 3 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?

- 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