



# Measurement Framework for SwA and Information Security

Nadya Bartol, Booz Allen Hamilton – Moderator  
Sean Barnum Cigital  
Bob Martin, MITRE  
Peter Mell, NIST  
Ron Ross, NIST



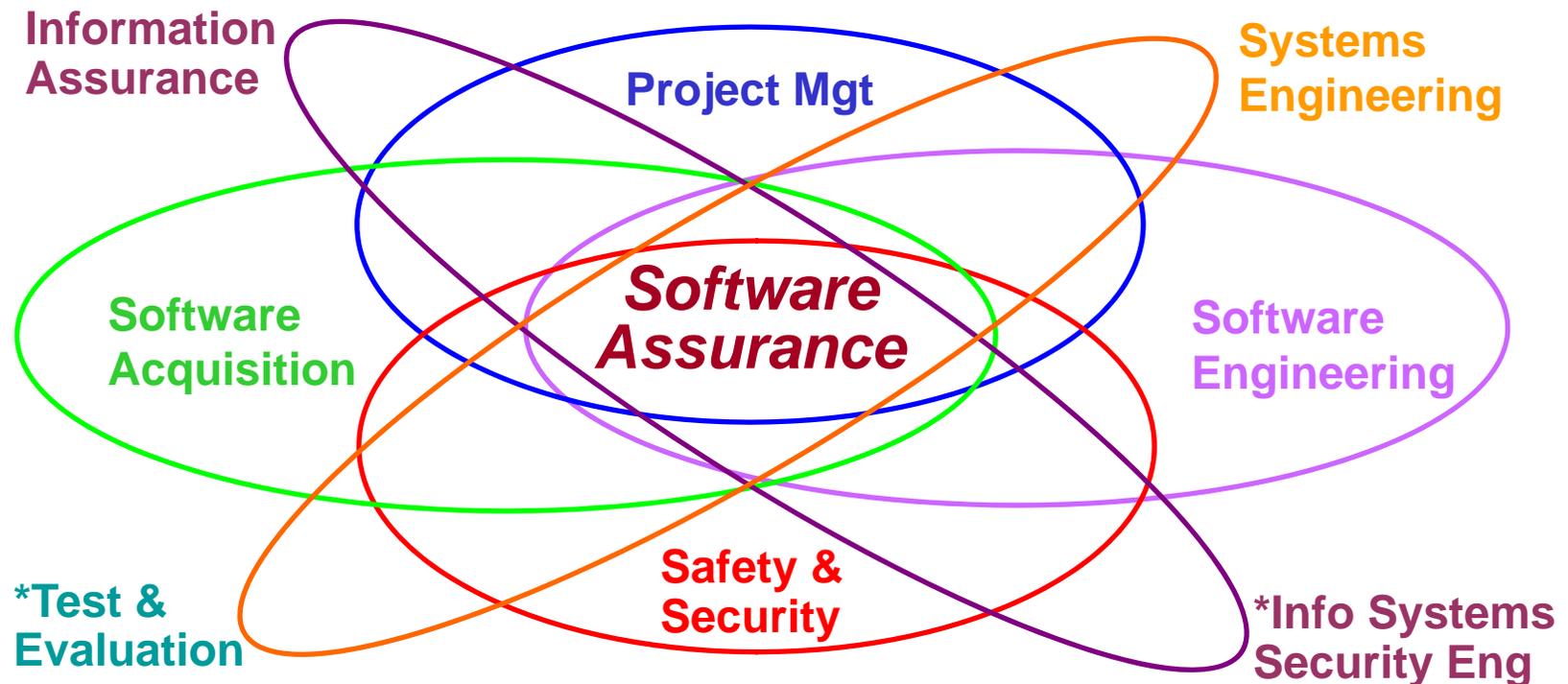
Homeland  
Security



- SwA Measurement Landscape
- CWE & CWSS and CAPEC
- Making Security Measurable
- SCAP, CVE & CVSS, and CCE & CCSS
- FISMA Risk Management Framework

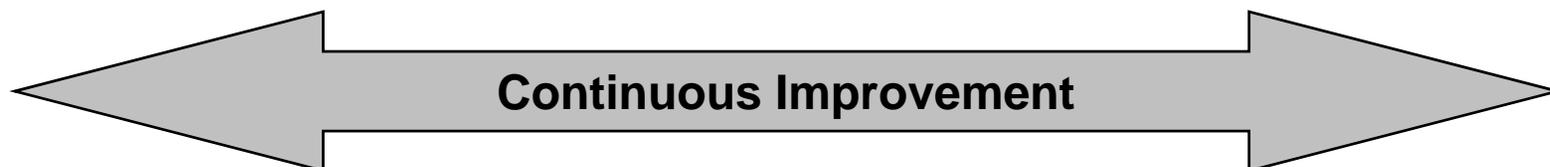


- New and evolving discipline
- Many people are working the problem from different angles
- Just like SwA, its measurement is not a standalone challenge





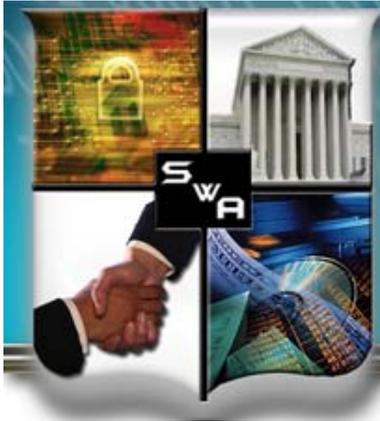
- Harmonized with five prevailing system/software and security measurement approaches
- Provides basic measures development and implementation processes
- Provides general measures examples
- Integrates with existing measurement programs
- Incorporates Making Security Measurable products
- Provides an overarching framework for summarizing SwA measures and communicating them to stakeholders





- **Enumerations of Things That We Want to Know About:**
  - Common Weakness Enumeration (CWE)
  - Common Attack Pattern Enumeration and Classification (CAPEC)
  - Common Vulnerabilities and Exposures (CVE)
  - Common Configuration Enumeration (CCE)
- **Ways of Expressing Details About Enumerated Items:**
  - Open Vulnerability and Assessment Language (OVAL)
  - XML Configuration Checklist Data Format (XCCDF)
  - Common Platform Enumeration (CPE)
  - Common Vulnerabilities Scoring System (CVSS)
  - *Common Configuration Scoring System (CCSS)*
  - *Common Weakness Scoring System (CWSS)*
- **Repositories of Content with Measurement Criteria**
  - SCAP (Secure Content Automation Protocol)

***Other measurable items include quality and project management measures which are well developed and available for use***



# SOFTWARE ASSURANCE FORUM

## BUILDING SECURITY IN

# Measurement and Risk Management

