Varying levels of Software Assurance initiative maturity

1. Sitting in the bleachers looking at the pool
2. Dipping toes into the Software Assurance pool
3. Wading up to their waist in the pool
4. Full-on swimming

- Lifeguards

- Most government organizations are between 1 & 2
- Many commercial organizations are between 2 & 3
- Several commercial organizations are at 4 but very few government organizations are there yet
- Most lifeguards are governmental

cigital

Lifeguards

- Develop and publish guidance, standards and knowledge resources for consumption and use by organizations building, buying and operating software.

- DHS NCSD Software Assurance Program
- DOD Software Assurance efforts out of OSD
- NSA Center for Assured Software
- NIST SAMATE & Trustworthy Information Systems

- A few commercial examples of experts like Cigital

cigital

Bleacher sitters and Toe dippers

- Bleacher sitters
  - Typically not in the game for one of four reasons:
    - Don’t understand SwA impacts them
    - Feel that it is someone else’s job
    - Lack proper top-down – bottom-up balance
    - Interested but procrastinating
- Toe dippers
  - Usually lack policy or top-down support
  - Typically start with pen testing or static analysis
  - Understand SwA to be synonymous with the perspective they know
  - Typical initiative age = 0-2 years
  - Fastest growing group

cigital

Waders & Swimmers

- Waders
  - Proven tactical successes
  - Looking to address other parts of the problem
  - Tackle multiple technical perspectives
  - Typical initiative age = 1-4 years

- Swimmers
  - Strategically address all aspects of SwA
  - Enterprise scope
  - Tackle technical, business and people dimensions
  - Rare (only 1 in gov't and ~25 in industry)

cigital

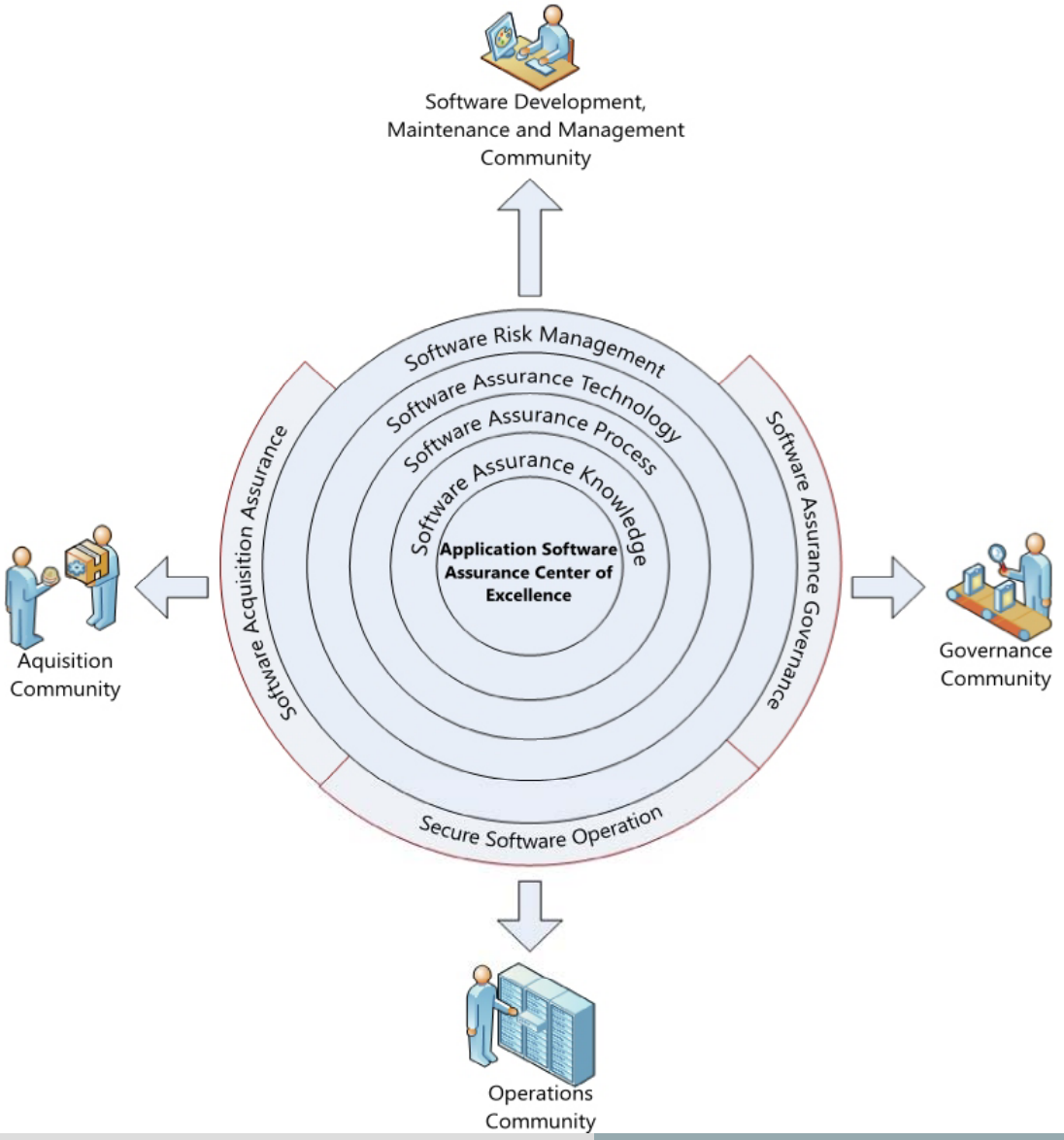
USAF Application Software Assurance Center of Excellence (ASACoE)

- Mission is to be the Focal Point for Air Force Software Assurance (SwA) capability with the goal of reducing software-induced risk from Air Force applications.
- Stood up in Aug 2007 as a reaction to the breach of an AF system
- Decision to address the root causes of problems rather than just patch the symptoms
- ASACoE structure
  - Blended teams of organic AF staff and expert contractors
- ASACoE Approach
  - Inform (evangelism, training and mentoring)
  - Enable (tools, techniques and knowledge)
  - Support (assistance and guidance)

cigital

USAF ASACoE Strategic CONOPS

- Provide expert guidance and support on software assurance issues to all relevant stakeholders throughout AF
- Address the full range of required SwA capabilities
- **Think Strategically**
- **Act Tactically**



A Few Accomplishments to Date

- Stood up 15 September 2007
- Defined Strategic CONOPs and tactical assessment procedures
- Identified 2,588 Government Off the Shelf applications
- Actionable data collected from >200 applications to date
- Conducted Assessments on >150 applications (>40 PMOs)
- Continuing to collect application information
- Working with SAF/AQ/XC to incorporate application software assurance language into contracts
- Working with 643ELSS to incorporate into Systems Engineering Process (SEP)
- Training and enablement of 643ELSS test group and 46th Test Wing

cigital

Leading commercial SwA Initiatives

- Building Security In Maturity Model (BSIMM) pulls together a set of activities practiced by nine of the 25 most successful software security initiatives in the world

http://www.bsi-mm.com

(and two unnamed financial services companies)

cigital

Data collection (Anthropologists unite!)

- Big idea: stop hypothesizing, study successful organizations
- Create a software security framework
- In-person executive interviews
- Build bullet lists (one per practice)
- Bucketize the lists to identify activities
- Create levels
  - Objectives → Activities
  - 110 activities supported by real data
  - Three levels of “maturity”

cigital

The Software Security Framework (SSF)

Governance	Intelligence	SSDL Touchpoints	Deployment
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Management

http://www.informit.com/articles/article.aspx?p=1271382

cigital

Real-world data

- Age: 5.3 yrs
  - Newest: 2.5
  - Oldest: 10
- SSG size: 41
  - Smallest: 12
  - Largest: 100
  - Median: 35
- Satellite size: 79
  - Smallest: 0
  - Largest: 300
  - Median: 20
- Dev size: 7750
  - Smallest: 450
  - Largest: 30,000
  - Median: 5000

Average SSG size: 1% of dev

cigital

Common ground

- Everyone has a software security group (SSG)
- SSG is roughly 1% size of dev team
- Ten activities that ALL do
  - evangelist role
  - policy
  - awareness training
  - history in training
  - security features
  - static analysis
  - SSG does AA
  - black box tools
  - external pen testing
  - good network security

http://www.informit.com/articles/article.aspx?p=1326511

cigital

For more info

Sean Barnum
Principal Consultant
Cigital Federal, Inc.
sbarnum@cigital.com
703-473-8262