



# HQ 754<sup>th</sup> Electronic Systems Group

---



## Application Software Assurance Center of Excellence (ASACoE)

Maj Michael Kleffman, CTO  
ASACoE



# Overview

---



- Context and Mission
- Resources and Tempo
- Accomplishments
- Services
- Current Findings
- Conclusion



# Context and Mission

---

- Today's Air Force relies heavily on software technologies to ensure the safety and security of the Warfighter
  - These software technologies are under an increasing risk of attack and exploitation
- The ASACoE seeks to thwart application-level compromises of government developed/acquired and maintained Automated Information Systems (AIS) and Combat Information Systems (CIS)
  - The center's Primary objective is designed to help the Air Force achieve cyberspace dominance by improving upon the assurance of combat and mission support applications and their underlying data

Delivering Knowledge, Processes, and Tools



# Resources and Tempo

---



- \$75M Contract
  - \$10.6M Obligated – FY 08
  - \$6.5M Obligated – FY 09
- Staffing
  - 14 Organic Personnel
  - 11 Full-Time Contractors
  - 4 Part-Time Contractors
- Teams Consist of 2 Organic & 2 Contractors
- 6 – 8 Assessments per Month



# Accomplishments

---



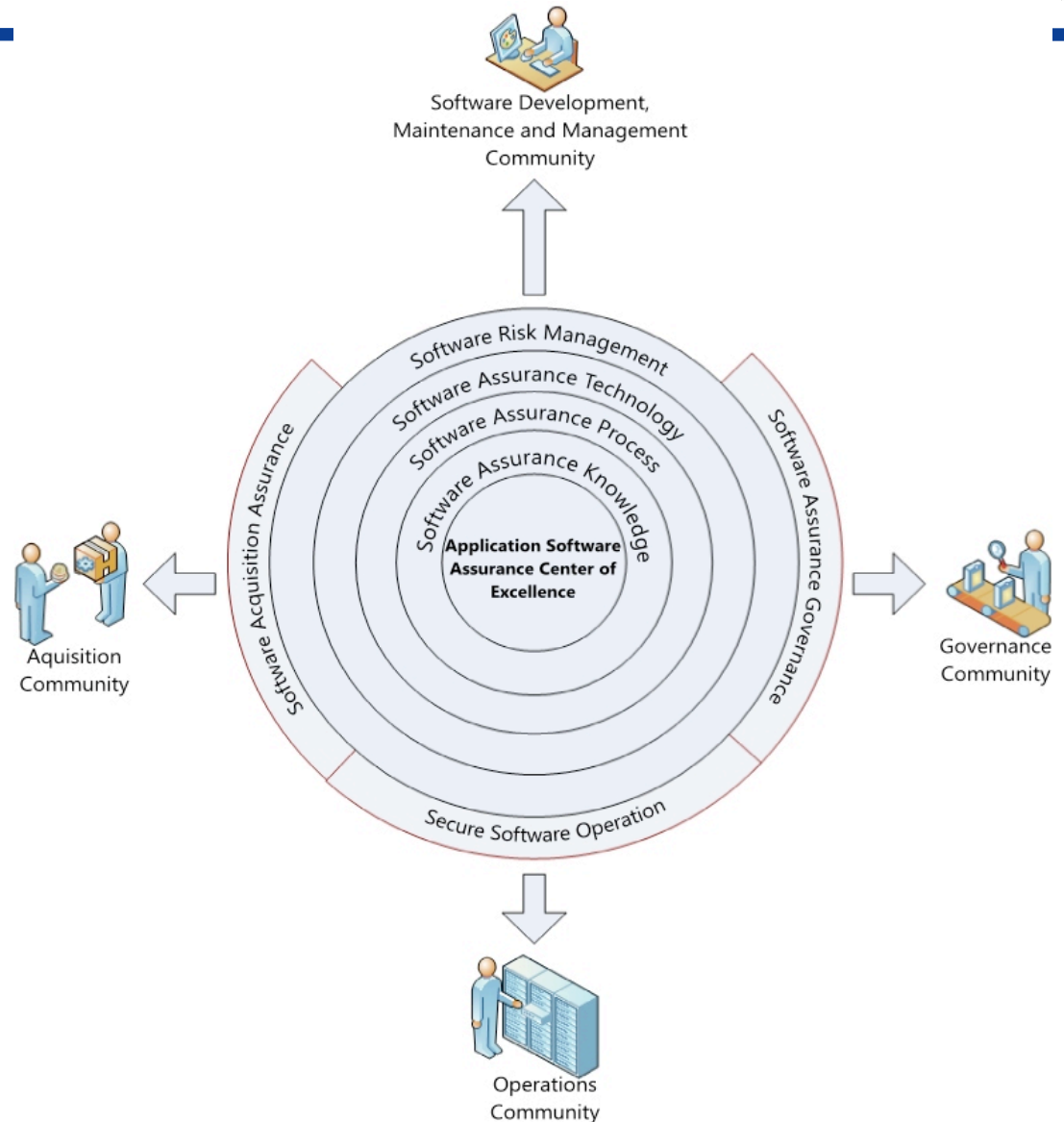
- Stood up 15 September 2007
- Identified 2,588 Government Off the Shelf applications
- Actionable data collected from >200 applications to date
- Conducted Assessments on >150 applications (>35 PMOs)
- Continuing to collect application information
- Working with SAF/AQ/XC to incorporate application software assurance language into contracts
- Working with 643ELSS to incorporate into Systems Engineering Process (SEP)



# 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**





# Services



- Triage Risk Assessment
  - 3 days of training
  - 2.5 days of tool installs and scanning
  - 5 days of analysis and mentoring at Gunter
  - 5 days of analysis and assessment report writing
- Training and Tools (No Assessment)
  - 3 days of training
  - 2.5 days of tool installs
- Assessment only (No training and no tools)
  - 5 days of scanning and analysis
  - 3 days of assessment report writing
- Detailed Risk Assessment
- Application Shielding and Data Monitoring
- Testing Organizations



# Training



- Class Size – 12 – 20
- PMO Courses
  - Defensive Programming (1 day)
  - Fortify SCA (1 day)
  - AppSec Inc. AppDetective (1/2 day)
  - Fortify Manager and RTA (1/2 day)
- Testing Organizations Courses
  - Security Testing (1 day)
  - IBM Rational AppScan (1 day)
  - SCA, AppDetective, Manager, & Fortify PTA
- Location
  - Gunter – 1 week per month
  - On-site – Combine multiple program offices if necessary



# Deliverables



- Mentoring
  - Provides Biggest Bang for Buck
  - Analyze Tool Results
  - Secure Coding Best Practices
  - Answer Security Related Questions
- Report
  - Snapshot in Time of Application Health
  - Prioritizes Findings
  - Provides Mitigation Recommendations for Findings
  - Top Weaknesses and Mitigation Recommendations
- Follow-up Support
  - Field Assistance Service Team 6
  - ASACoE
  - Vendors via ASACoE



# Brief Sampling of What We Have Found So Far



- Every application assessed has been vulnerable
- Top eight issue types found through tool scans account for 84% of issues flagged
  - **Cross-site Scripting (XSS) (31%)**
  - **SQL Injection (27%)**
  - Trust Boundary Violation (Excessive Privilege) (5%)
  - Log Forging (5%)
  - System Information Leak (4%)
  - Access Control: Database (4%)
  - Poor Error Handling (4%)
  - Missing Check Against Null (4%)
- Across a group of 35 related small applications
  - Average number of findings = 2661
  - Average SLOC = 28430
  - Average lines of code per finding = 10
  - Average percentage of findings analyzed = 28



# Conclusion

---

- Our apps are vulnerable today -- the threat is growing
- Needs focus throughout Software Development Lifecycle
- Need combination of tools and processes
- Collaborative effort with Cyber Command
- Our goal is to institutionalize software assurance across our enterprise



# POCs



- PM
  - Mr. Dan Bartko  
754th ELSG/DOC  
[daniel.bartko@gunter.af.mil](mailto:daniel.bartko@gunter.af.mil)
- Chief Technology Officer
  - Capt Michael Kleffman  
754th ELSG/DOC  
[michael.kleffman@gunter.af.mil](mailto:michael.kleffman@gunter.af.mil)
- Assessment Teams Chief
  - James Woodworth  
754th ELSG/DOC  
[james.woodworth@gunter.af.mil](mailto:james.woodworth@gunter.af.mil)