# Independent Software Quality Assessment (ISQA) Services: *Makes Dollars and Sense*

## Presented to the Systems & Software Technology Conference Salt Lake City, UT

**Edward J. Dlugosz**

**I-SQA Special Projects Office**

**Software Engineering Center**

edward.dlugosz@us.army.mil

# OVERVIEW

- Who is SEC?
- What is ISQA?
  - What is NOT ISQA
- Why?
  - Software Costs
  - Benefits of ISQA
  - ISQA Services
- When?
  - Throughout Life Cycle
  - Proven Examples
- How?
  - Processes
  - Enterprise Solution
- Summary

# Who is Software Engineering Center?

**MISSION**

**SEC Supports**

**Deliver life cycle software solutions that ensure warfighting superiority and information dominance**

**BENEFITS**

- **Enterprise view**
- **Continuity of support over the life-cycle**
- **Army/Joint/Allied interoperability**
- **Rapid application of technology to Current Force**
- **Integrated world-wide field support for software**

**COST EFFECTIVE**

**INTEGRATED**


**INNOVATIVE**

**SUPERIOR**

PEO-EIS — CECOM — PEO-C3T — PEO-IEW&S — CERDEC

COMMUNICATIONS ELECTRONICS LIFECYCLE MANAGEMENT COMMAND

# Who is SEC?

## *Support For Battlespace & Business Systems*

- **Provide software engineering support for Program Executive Offices and their respective Program Managers, DoD/Army Functional Proponents and the CE-LCMC**
  - **System Software and Application Development**
  - **Technical Support**
  - **Acquisition Support**
- **Provide Post Deployment/Production Software Support (PDSS/PPSS) for deployed Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance (C4ISR) systems & enterprise information systems.**
  - **Maintain system's minimum essential warfighting capability**
  - **Significantly improve system's warfighting capabilities**
- **Provide Replication, Distribution, Installation and Training services.**
- **Provide Integrated Field Software Engineering support.**
- **Provide worldwide customer assistance through our Global Support Center**
- **Apply advanced technology to meet current needs.**
- **Implement SQA through our ISQA Team**
  - **Dedicated Cadre of computer scientists/engineers with access to hundreds of SEC assets. The Team consists of Government and SQA Contractors who can quickly complement our Government cadre's expertise and supplement our capacity with proven SQA performers**

**Major customers:**

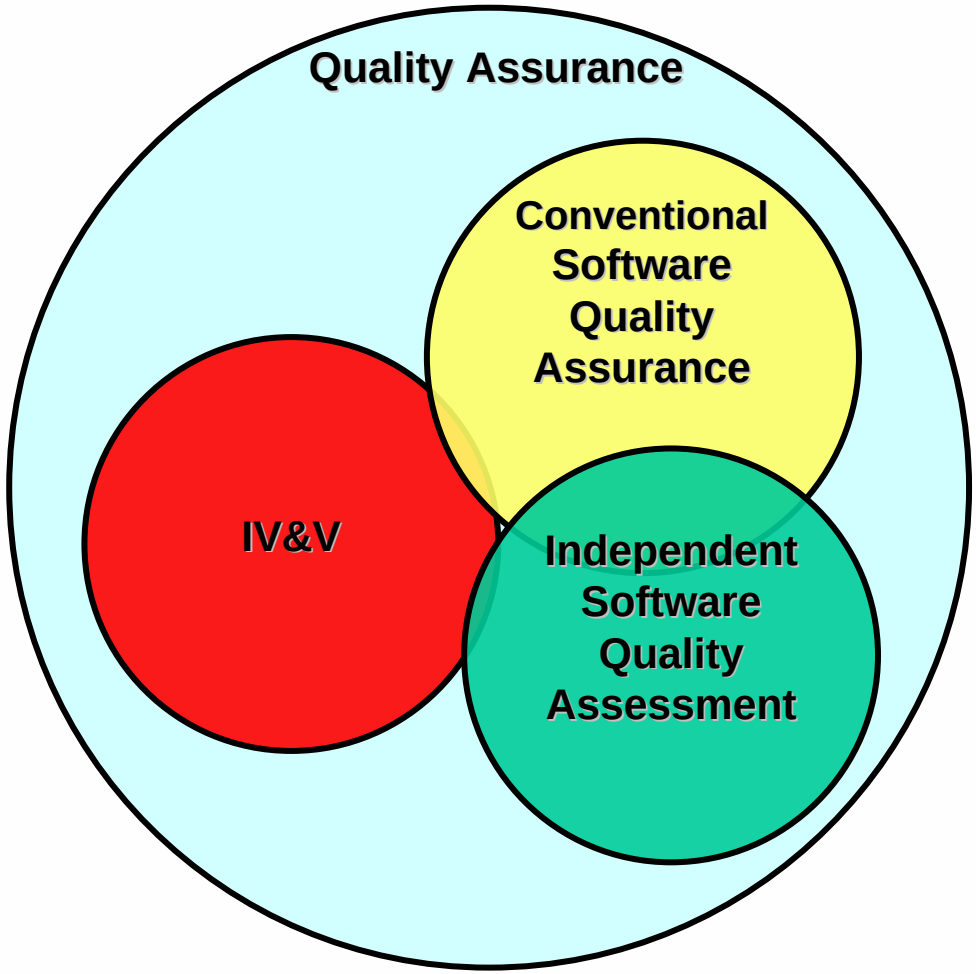
- PEO C3T
- PEO IEWS
- PEO EIS
- JPEO JTRS
- Other PEOs
- DA Staff
- DOD/Agencies
- Other Services

# What is ISQA?

1. Independent Software Quality *Assessment* is an SEC Initiative to improve Army's Software Business
2. ISQA is a combination of objective methods, tools, and techniques that are used to assess the various quality attributes of software products at various stages in their development and provide recommendations for improvement.
3. Quality Attributes include:
   - Correctness
   - Reliability
   - Performance
   - Adaptability
   - Robustness
   - Usability
   - Eliminate System Vulnerabilities
   - Maintainability
   - Portability
   - Safety
   - Interoperability
4. ISQA Team will provide the Army & DOD community with a broad spectrum of software assessment services to ensure software quality throughout the life cycle development process.

# ISQA is Not

- Independent Verification & Validation (IV&V):
  - Does Not Verify That Requirements Are Implemented
  - Does Not Validate That The System Functions Correctly
- Conventional Quality Assurance Of Software
  - Not Observations Of Processes Or Activities
  - Not Documentation Or Plans Which Promise Adherence To Standards And Models
  - Not Formal Developmental Test Nor Operational Test



# Software Costs

## *Industry- & DOD-wide*

**$8B out of $15B (40%) spent on software in 2003 went to reworking software because of Quality-related issues**

*(Stronger Management Practices Are Needed, GAO Mar 2004)*

- **"Finding and fixing a software problem after delivery is often 100 times more expensive than finding and fixing it during the requirements and design phase." is still a valuable heuristic according to Barry Boehm and legions of colleagues while discussing the software costs and risks of large software projects…"**

  **(Barry Boehm, March 16, 2001)**

- **As a rule of thumb, every hour you spend on defect prevention will reduce your repair time from three to ten hours.**

  **(Boehm and Papaccio 1988)**

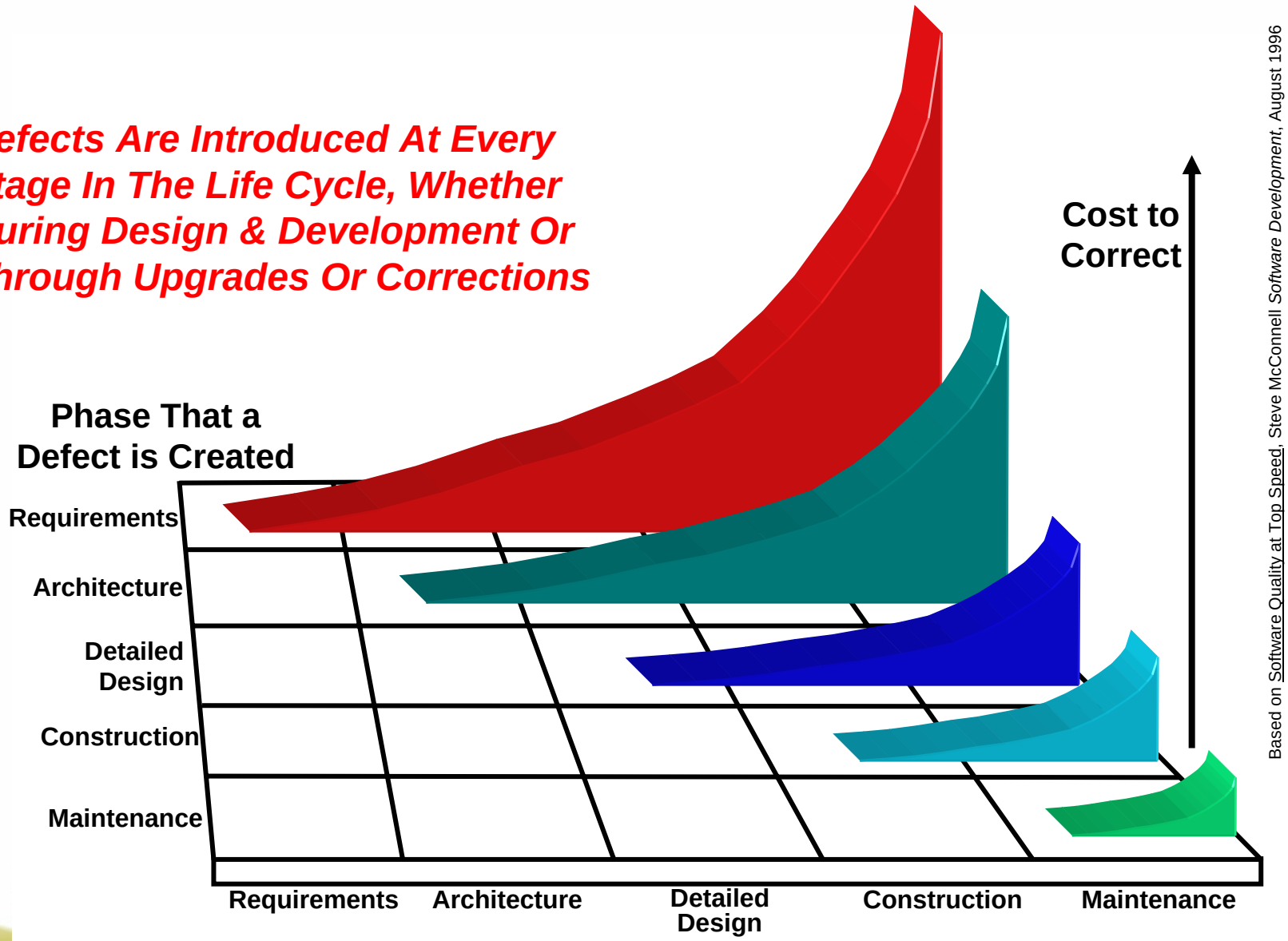
- **28%** projects expected to finish on-time, within budget
- **40%** projects cancelled before completion
- **$145B** spent on cancelled projects
- **50%** of projects will cost nearly twice original estimate
- **42%** of originally proposed features actually implemented

*(CHAOS Report 1994: ©Standish Group)*

# Software Costs

## *Defect Correction: The Sooner the Better*

***Defects Are Introduced At Every Stage In The Life Cycle, Whether During Design & Development Or Through Upgrades Or Corrections***




Based on Software Quality at Top Speed, Steve McConnell *Software Development*, August 1996

# SQA Services

## *Targeted at Providing Meaningful Software Quality*

### Software Vulnerability Analysis

Provides analysis of source and/or binary code or runtime application for security vulnerabilities--intentional or inadvertent. Malicious code analysis and penetration testing which can be made available based on customer request.

### Error Detection

Provides source code and dynamic analysis for errors/bugs or violations of software coding practices. Identifies problems by severity and importance. Recommend remediation courses of action.

### Performance Tuning

Identifies design or coding practices or implementation issues application that adversely impact performance and response times Recommends remediation that result in significant performance improvements and response times.


### Test Coverage Analysis

Provides analysis of effectiveness of the system testing by determining the test coverage. Identifies where the developmental/ user test procedures are redundant or testing is insufficient.

### Memory Leak Analysis

Identifies system memory resources problems & provide an assessment of & recommendations for specific and overall system performance degradation caused by memory leaks.

### SCA Assessment

Identifies source code elements that are incompatible with the SCA standards & assess their impact to the proposed SCA compliant application.

### COE Assessment

Analysis of the source code & development artifacts to identify characteristics of systems that are non-compliant to the Common Operating Environment standard or unsuitable for running on the COE

### Preliminary Quality Assessment

Provides an overall, high-level insight of the general health of the system by reviewing Quality Assessment (QA) specific metrics, . QA metrics will include various categories of information about the system such as size, depth, complexity, structure, defects, faults, and errors. The Preliminary Assessment will help determine if further testing is needed. Extended Metrics can be made available based on customer request.

# Benefits of ISQA Services

## *SEC Enterprise Service*

- Provides an objective perspective on the “goodness”, efficiency and confidence of the software product.
- Analysis/Audit is Independent from the Prime Contractor.
- Provides alternative methods, repeatable processes, & ways to measure/assess software, solve problems, and mitigate risks.
- Motivates Software Developers to be more diligent in coding, code inspections and testing the software.
- Identifies Software Problems – which can be fixed earlier while under development contract/warranties.

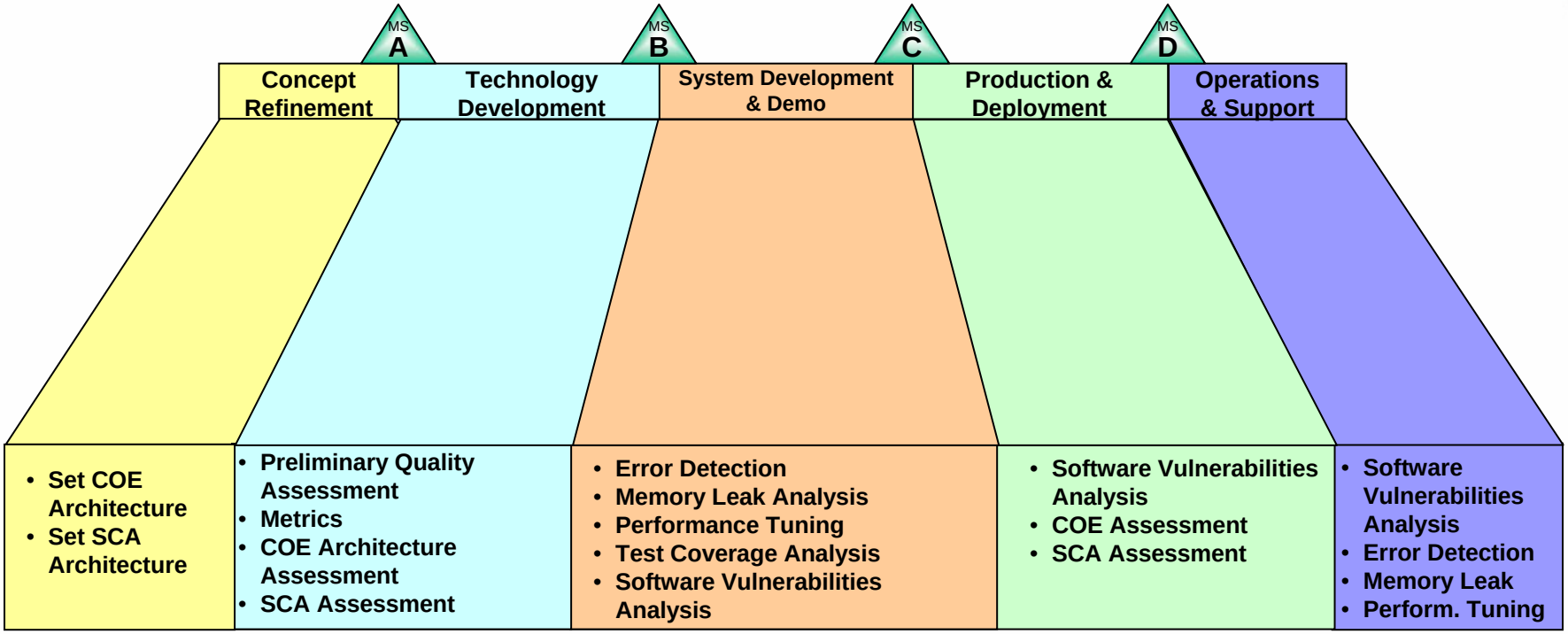
# Benefits of ISQA Services

*SEC Enterprise Service*

- **Leverage Proven SEC Enterprise Service Processes:**
  - **Certification and Accreditation (C&A)**
  - **Malicious Code Analysis (MCA)**
  - **Global Service Center (GSC)**
  - **Replication, Distribution, Installation & Training (RDIT)**
- **Benefits All Systems**
  - **Tactical/Strategic**
  - **Sustaining Base**
  - **Business**
- **Provides Value to Customer**
  - **Provides that "missing" insight**
  - **Reduce Overall Costs**
  - **Improved Results**

# SQA

## *Synergies With the Acquisition Life Cycle*

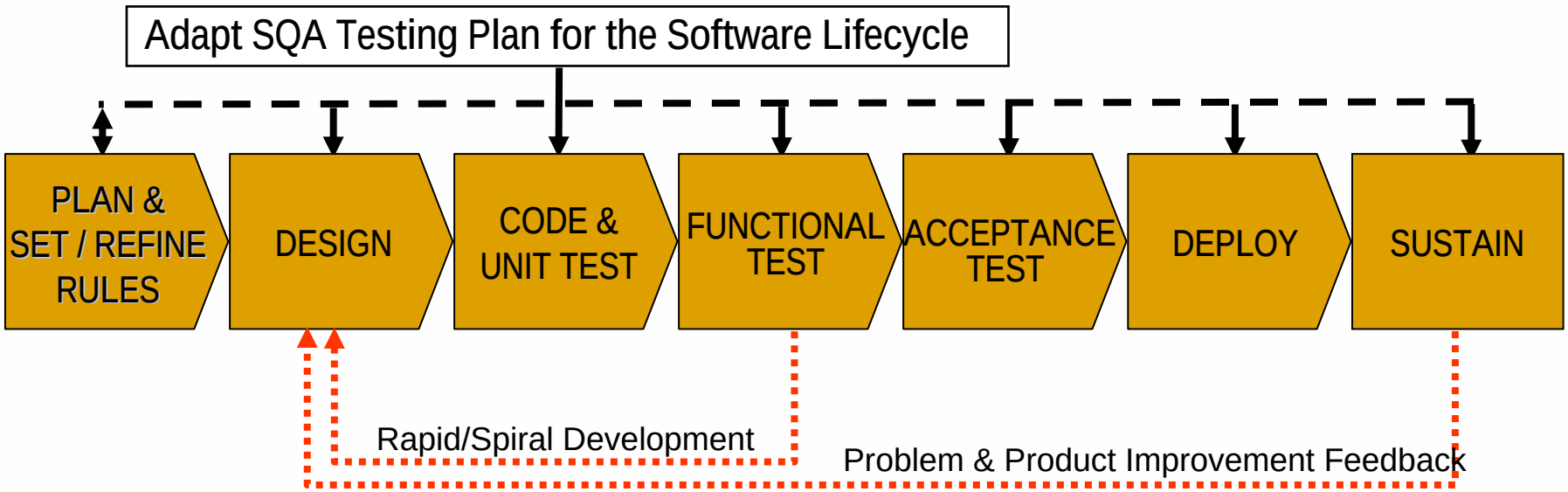



- Independent SQA services are recommended at appropriate phases of the Acquisition Life Cycle
- Appropriate Independent Software Quality Assessments are recommended at Milestones (MS) B, C and D

# Software Quality Assessment

## *Throughout the Software Life Cycle Process using Enterprise Tools*

- Eliminate Errors, Performance Bottlenecks, And Vulnerabilities When Least Costly
- Automatically Capture & Maintain Results For Remediation, Compliance, Trending, & Secure Quality Assurance
- At Minimum, Perform SQA Tests At Major Builds And Re-deployments
- Results in Built-In Protection and CMMI Process Improvement



# Proven Examples:

## *Past Government Customers*

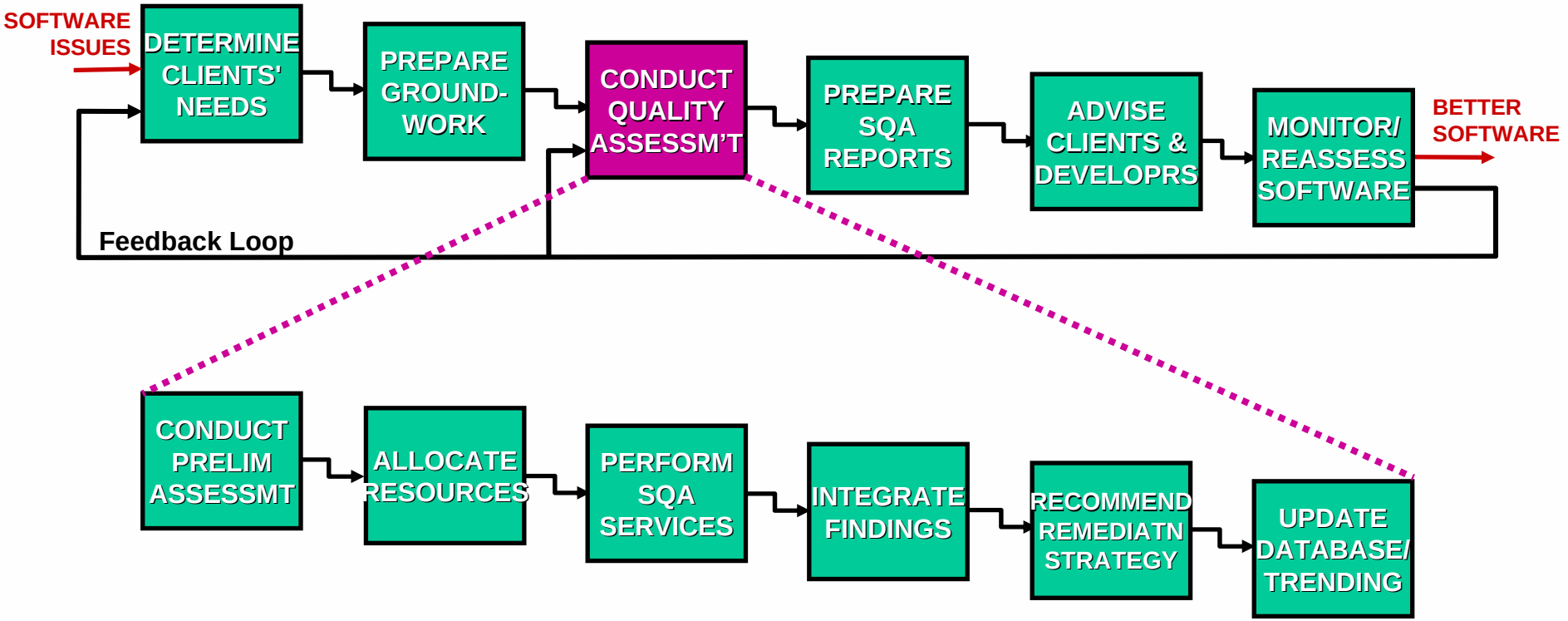
- **Joint Tactical Terminal**
- **Guardrail**
- **Common Ground Station**
- **Agile Commander**
- **MCS Light & Heavy**
- **Electronic Key Management System (EKMS)**
- **JTRS Soldier Radio Waveform**
- **RFMOW**
- **MCS NRTS**

# Current & Near-Term Future Customers

- GCCS(A) - PM GCCS (A)
- MCS NRTS-PASS
- Joint Tactical Radio System (JTRS) - JPEO JTRS
- ATIRCMS CMWS - PM AES
- Financial Disclosure Management (FDM)
- WIN-T - PM WIN-T
- DCGS-A - PEO IEW&S
- Key Management Infrastructure (KMI)
- Simulation, Training, & Instumentation Systems - PEO STRI

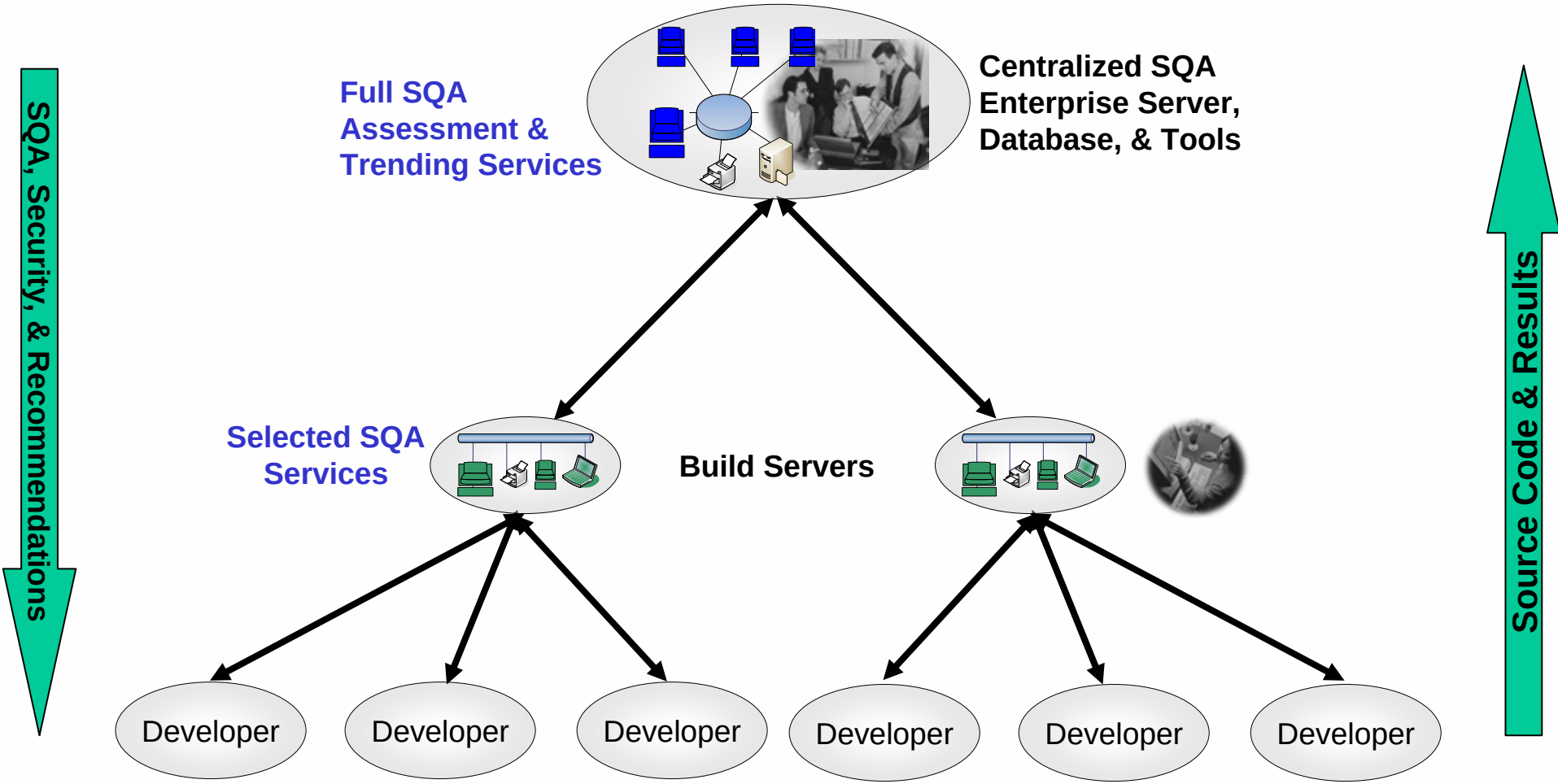
# Integrated Defense System Life Cycle Management Framework

## *ISQA Process Supports Software Life Cycle*



# SQA Enterprise Solution

*Distributed SQA Tools for Early Detection and Remedy*




SQA Needs to Be Established as Standard Part of S/W Acquisition

PEO-EIS — CECOM — PEO-C3T — PEO-IEW&S — CERDEC

COMMUNICATIONS ELECTRONICS LIFECYCLE MANAGEMENT COMMAND

# Summary

- ISQA is a new US Army CE LCMC SEC initiative
- ISQA is part of SEC's Enterprise approach to software
- Use of ISQA will reduce costs and schedules
- ISQA can benefit US Warfighters by improving software quality which provides:
  - Increased reliability and availability
  - Improved response times and performance
  - Improved security:  protection against vulnerabilities & malicious code and increased information assurance
  - Improved interoperability and portabililty

# SEC Single Point of Contact

**Thomas Spinelli**
**ISQA Special Projects Office**
**Information Technology Enginering Directorate (ITED)**
**Software Engineering Center**
**Building 1209, Room 330**
Thomas.Spinelli@us.army.mil
732-532-6881

# SQA Services

## *Preliminary Quality Assessment*

**Provides an overall, high-level insight of the general health of the system by reviewing Quality Assessment (QA) specific metrics, . QA metrics will include various categories of information about the system such as size, depth, complexity, structure, defects, faults, and errors. The Preliminary Assessment will help determine if further testing is needed. Extended Metrics can be made available based on customer request.**


### Typical Defects/Issues Discovered

- Overly complex code which is prone to errors & insufficient remediation
- Maintainability and architecture issues
- Bad coding practices
- Possible defects and vulnerabilities

### Benefits

- Quick turnaround report of general system health to customer
- Defines areas needing closer examination
- Permits drill-down for identification & verification of defect or issue
- Lower Cost

# SQA Services

## *Software Vulnerability Analysis*

**Provides analysis of source and/or binary code or runtime application for security vulnerabilities--intentional or inadvertent. Extended vulnerabilities testing including malicious code analysis and penetration testing which can be made available based on customer request.**


### Typical Defects/Issues Discovered

- Weak Encryption Methods
- SQL Injections and Path Manipulation
- Vulnerabilities & data corruption caused by memory overflow
- Security vulnerabilities caused by bad coding practices
- Control & Data Flow Exploitation

### Benefits

- Greater system availability and non-repudiation
- Assured Data Integrity
- Trusted System

# SQA Services

## *Error Detection*

Provides source code and dynamic analysis for errors/bugs or violations of software coding practices. Identifies problems by severity and importance. Recommend remediation courses of action.


### Typical Defects/Issues Discovered

- Semantic Vulnerabilities beyond Compiler Checking
- Unreleased Resources
- Redundant or Unused Code, Classes, and Methods
- Null references
- Bad Coding Practices

### Benefits

- Improve Reliability & Availability
- Improve Performance
- Strengthen Coding Practice Guidance
- Early Detection Reduces Cost Dramatically

# SQA Services

## *Performance Tuning*

**Identifies design or coding practices or implementation issues that adversely impact performance and response times  Recommends remediation that result in significant performance improvements and response times.**


### Typical Defects/Issues Discovered

- Unreleased Resources--Memory, Sockets, Control, Processing
- Redundant or Unused Code, Classes, and Methods
- Bottlenecks within and among systems, modules, methods
- Run-time, Dynamic Problems

### Benefits

- Higher Performance
- Increased Response Times
- Streamlined, Efficient APIs
- User Buy-in and Confidence

# SQA Services

## *Memory Leak Analysis*

**Identifies system memory resources problems & provides an assessment of, and recommendations for, specific and overall system performance degradation caused by memory leaks.**


### Typical Defects/Issues Discovered

- Lack of Allocation/De-Allocation Pairing
- System Crashes and Unavailability
- Unreleased Resources--Memory, Sockets, Control, Processing
- Performance Degradation & Data Corruption

### Benefits

- System Availability
- Performance Increases
- Lessens Security Vulnerabilities

# SQA Services

## *Test Coverage Analysis*

**Provides analysis of effectiveness of current system testing by determining the test coverage. Identifies where the developmental/user test procedures are redundant or testing is insufficient.**


### Typical Defects/Issues Discovered

- Full Range of Errors, Defects and Vulnerabilities due to lack of test coverage
- Unexpected Errors after Rigorous User Testing
- Uncertain, Unstable Program Control

### Benefits

- Greater Confidence in Developmental and User Testing
- Reduced Overall Costs by Catching Errors Sooner
- Faster, Reliable Testing Schedule

# SQA Services

## *SCA Assessment & Audit*

**Identifies source code elements that are incompatible with the SCA standards & assess their impact to the proposed SCA compliant application.**


### Typical Defects/Issues Discovered

- Incomplete Transmission and Receipt of Expected Data
- Interoperability Issues
- Portability Issues
- Performance Issues
- Security Issues

### Benefits

- Minimize Risks & Achieve:
  - Expected Interoperability
  - Expected Portability
  - Expected Performance
  - Fuller Reusability

# SQA Services

## *COE Audit & Assessment*

**Analysis of the source code & development artifacts to identify characteristics of systems that are non-compliant to the Common Operating Environment standard or unsuitable for running on the COE**


### Typical Defects/Issues Discovered

- Competition for Usage of Same Resources--"Dueling Pointers"
- Redundant Code & COTS Software
- Interoperability Issues
- Portability Issues
- Performance Issues

### Benefits

- Compatibility among Systems on Same Platform
- Minimize Risks & Achieve:
  - Expected Interoperability
  - Expected Portability
  - Expected Performance
  - Fuller Reusability