21st Annual National Defense Industrial Association
Systems and Mission Engineering Conference

Joint Federated Assurance Center (JFAC): 2018 Update

Thomas Hurt

Office of the Under Secretary of Defense for
Research and Engineering

October 24, 2018

Distribution Statement A: Approved for public release. Distribution is unlimited. DOPSR Case #19-S-0017

What Is the JFAC?

FY14 NDAA Section 937 — Joint Federated Assurance Center (JFAC)

It is the federation of capabilities to support the trusted defense system needs of the Department to ensure security in the software and hardware developed, acquired, maintained, and used by the Department.

Key provisions of Sec 937:

- Develop JFAC Charter for DEPSECDEF issuance
- Build DoD-wide federation of assurance capabilities
- Assure resilience and security in the **software** and **hardware** developed, acquired, maintained, and used by the Department
- Define software assurance (SwA) and hardware assurance (HwA) capability gaps
- Prioritize assurance initiatives based on what the gaps impact
- Report to Congress on funding, management, and place of JFAC in DoD

JFAC Charter elements:

- Role of federation in supporting program offices
- SwA and HwA expertise and capabilities of the Federation, including policies, standards, requirements, best practices contracting, training and testing
- Research and Development (R&D) program with DASD (R) for Assured Software to improve code vulnerability analysis and testing tools
- R&D program to improve hardware vulnerability, testing, and protection tools
- Requirements to procure manage, and distribute enterprise licenses for SwA and HwA engineering analysis tools

Distribution Statement A: Approved for public release. Distribution is unlimited. DOPSR Case #19-S-0017

JFAC Operational Structure

JFAC Steering Committee

- CIO / Army / Navy / Air Force / USMC / DISA / NSA / NNSA / NRO / DMEA / MDA
- Approve JFAC Strategic Plan

JFAC Action Officer (AO) Working Group

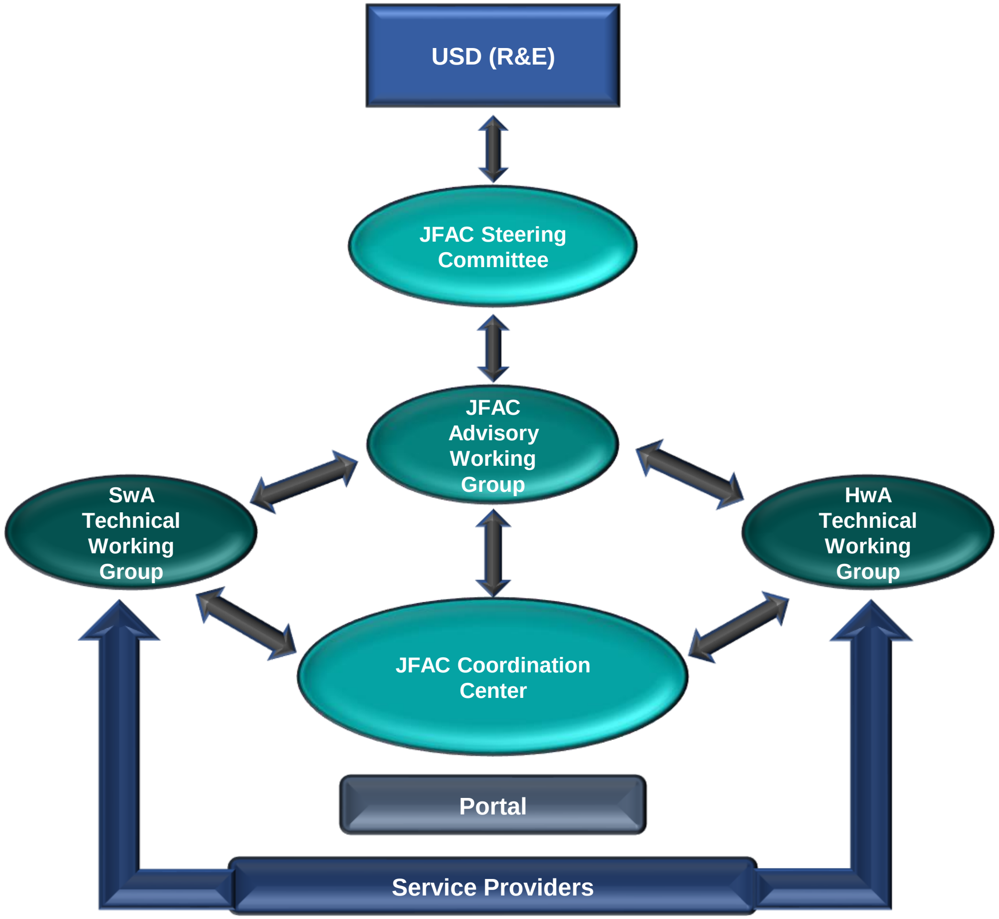
- AOs for JFAC Steering Committee
- Reporting, Strategic Planning, and budget Execution Analysis

SwA and HwA Working Groups

- Collaboration and shared prioritization in daily/weekly activities, meet on a regular basis
- Recommend policy and guidance
- Development of SwA/HwA artifacts

JFAC Coordination Center

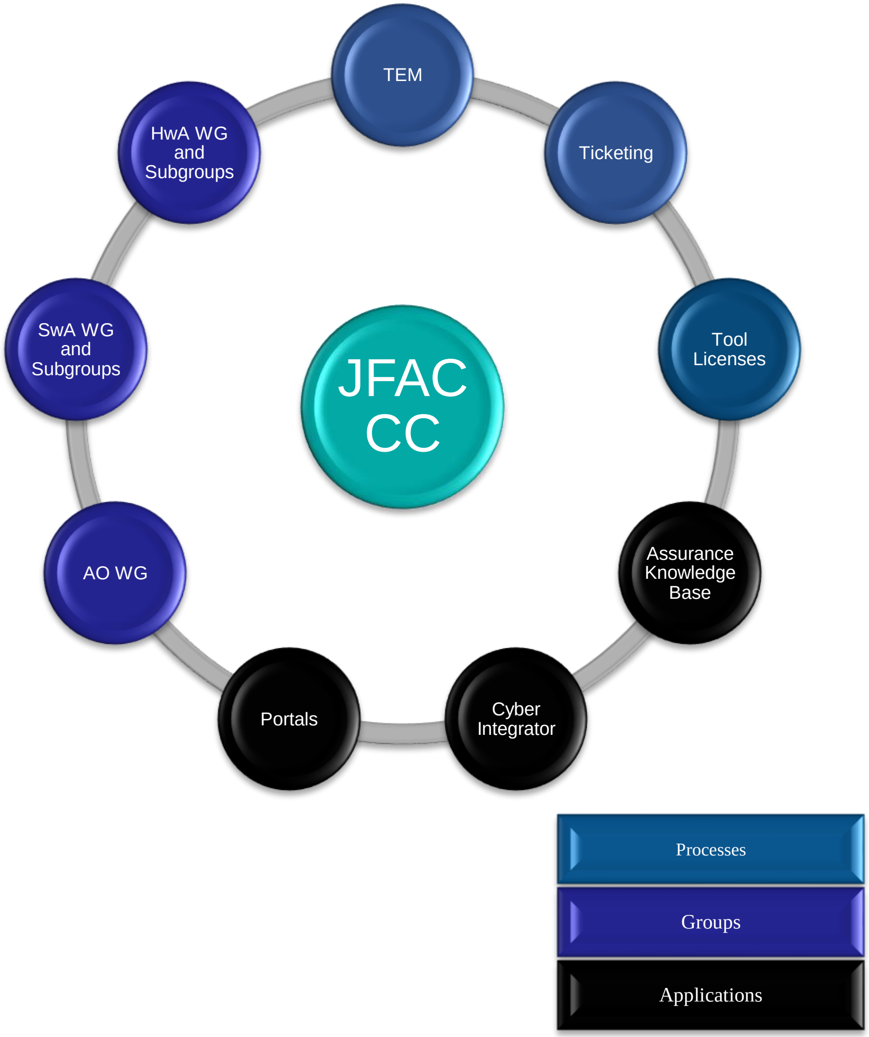
- Coordination of **Service Providers**
- **Portal:** https://jfac.navy.mil
- Maintain Assessment Knowledge Base and other JFAC tools


USD (R&E)
JFAC Steering Committee
JFAC Advisory Working Group
SwA Technical Working Group
HwA Technical Working Group
JFAC Coordination Center
Portal
Service Providers

Distribution Statement A: Approved for public release. Distribution is unlimited. DOPSR Case #19-S-0017

JFAC Activities

- Processes
  - Ticket and Response Coordination
  - License Coordination
  - **FOC Planning and Execution**
  - **DAU CLE 081 SwA Course Development**
  - **Security Classification Guide Development**
- Working Groups
  - Action Officer Working Group
  - Software Assurance Working Group
    - SwA Portal content sub-group
  - Hardware Assurance Working Group
    - Standards and best practice, FPGA, SCRM, Technical Assessment, ASSESS and EDA assurance sub-groups
  - **DAU/CSIAC Cybersecurity Experiment (CYBEX)**
- Applications
  - Cyber Integrator Development and Management
  - Portal Development and Management
  - AKB Development and Management
  - **S&T Portal Development**

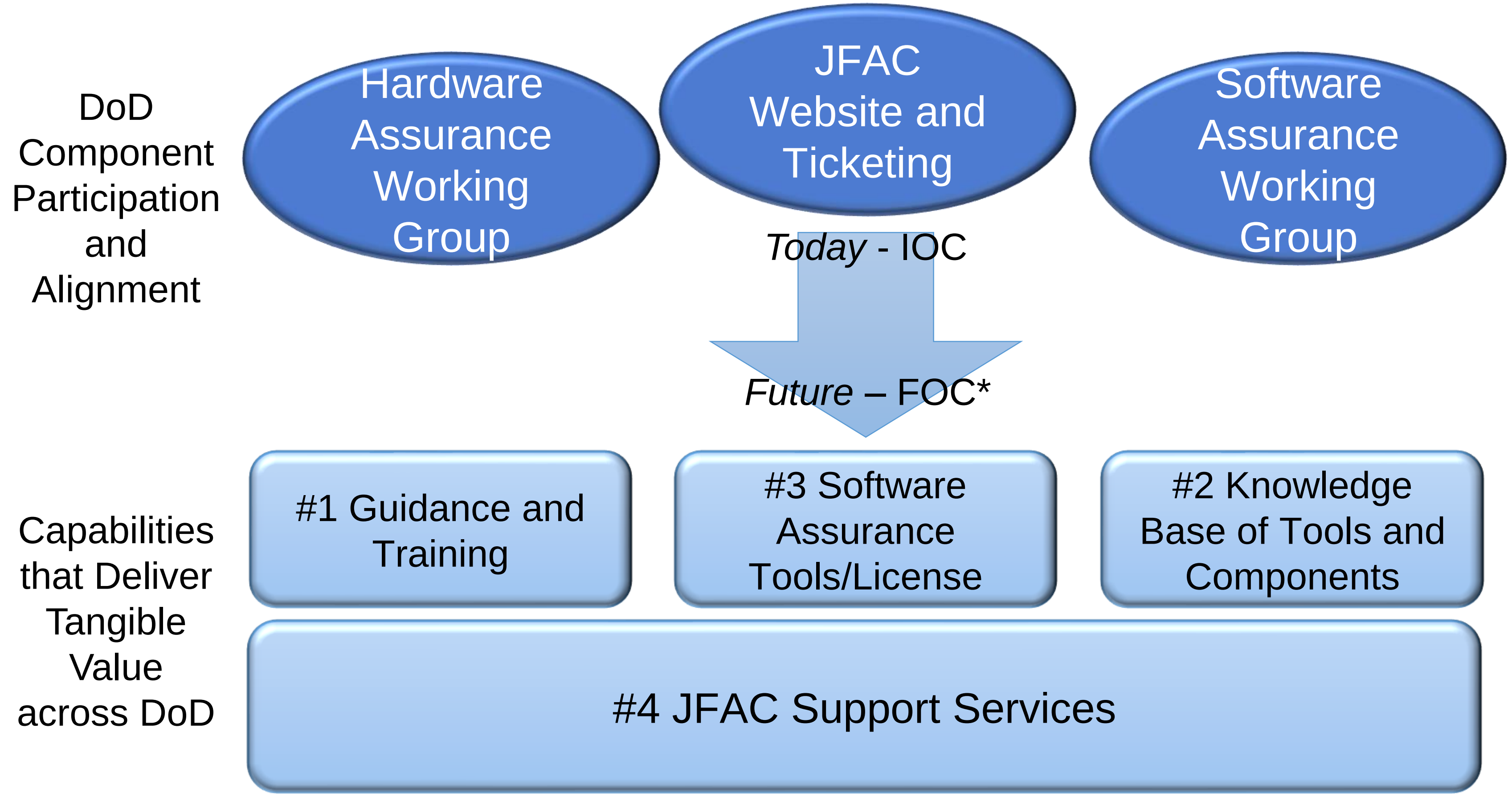


Distribution Statement A: Approved for public release. Distribution is unlimited. DOPSR Case #19-S-0017

JFAC Full Operational Capability (FOC) Plan

Plan meets requirements directed and defined by:

- NDAA Sec 937
- JFAC Charter and CONOPS
- DODI 5000.02
- DAU Chapter 9-4.5
- SwA Capability Gap Analysis



DoD Component Participation and Alignment

Hardware Assurance Working Group

JFAC Website and Ticketing

Software Assurance Working Group

Today - IOC

Future – FOC*

Capabilities that Deliver Tangible Value across DoD

#1 Guidance and Training

#3 Software Assurance Tools/License

#2 Knowledge Base of Tools and Components

#4 JFAC Support Services

*FOC subject to resources

#1 Guidance and Training

- **Problem**: Most PMs are unaware or inexperienced with current SwA standards and are consuming valuable time to plan and execute software development practices.
- **Objective**: Collect and publish SwA best practices, actionable guidance, training and pilot the guidance with programs
- **Deliverables**:
  - Lifecycle guidance for PMs
  - Contract language guidance
  - Training packages for PEO, PMs and SW professionals
- **Near Term Value**: Programs/projects can use JFAC resources to start from a common position, freeing time and resources that can focus on bigger project technical issues.

JFAC will distribute a Defense Acquisition University-like desk reference "The Silicon Card" that lists statutory/regulatory actions programs must take for Software Assurance and provide deeper links to JFAC training and guidance.

Distribution Statement A: Approved for public release. Distribution is unlimited. DOPSR Case #19-S-0017

#2 Knowledge Base of Tools and Components

- **Problem:** There are many choices available for code analysis. As a result, many software (SW) leads are unsure which tool to use and have never conducted formal SwA analysis.
- **Objective:** Establish and maintain a knowledge base of tools and evaluated components
- **Deliverables:**
  - Service Provider survey and gap results
  - SwA tool set evaluations
  - Pilot assessment of common open source software component using results from tool set evaluations
- **Near-Term Value:** Demonstrate the utility of top commercial static code analysis tools while concurrently providing those results on commonly used components.

JFAC will evaluate Red Hat Linux, the operating system of a significant percentage of DoD weapons systems, providing immediate benefit to any program utilizing those systems while giving insight on future Software Assurance analyses.

Distribution Statement A: Approved for public release. Distribution is unlimited. DOPSR Case #19-S-0017

#3 Software Assurance Tools

- Problem: Procuring “one-off” software places undue burdens upon project teams. Initial set-up and configuration can delay the start of coding activities by months.
- Objective: Make SwA tools affordable and easily obtainable
- Deliverables:
  - Enterprise-level license acquisition model available to all project sizes
  - Easy license distribution
  - Report from rapid acquisition pilot to assist in tool acquisition
- Near-Term Value: Provide smoother glide path and known-quantities for SwA tool procurement and use that can be reliably used in planning and project start-up activities.

JFAC will provide the tools for DoD software developers to easily and affordably create project development environments that can reduce project startup times by up to 6 months.

Distribution Statement A: Approved for public release. Distribution is unlimited. DOPSR Case #19-S-0017

#4 JFAC Support Services

- **Problem**: PEOs, Program Managers, Software Development Leads are unaware of JFAC's offerings.
- **Objective**: Enable JFAC Software Assurance capabilities through comprehensive and interconnected support services
  - JFAC Coordination Center
    - Bring initial users in and retain them with valuable information and services
    - Access to Assurance Knowledge Base
    - Ticketing support
    - License distribution
    - Connecting/supporting risk evaluations of critical components
  - Outreach: Ongoing Marketing, Technical Exchange Meetings
    - JFAC capability marketing
    - Feedback for JFAC "tuning" across all deliverable areas
- **Deliverable**: JFAC Web Portal 4.0
    - Fill website with content sourced from all JFAC capability areas
    - Develop new content based on user needs
    - Backend hosting on NIPR, SIPR and JWICS
- **Near-Term Value**: JFAC Web Portal 4.0 will become a coordinating center for easy one-stop activity.

Support services will be the glue that interconnects the DoD software community and enables JFAC's other three capabilities

Distribution Statement A: Approved for public release. Distribution is unlimited. DOPSR Case #19-S-0017

CLE 081
Software Assurance (SwA) Awareness
Continuous Learning Module (CLM)

Overview:

The CLE 081 SwA Awareness continuous learning module is intended for all DoD acquisition professionals, across all Services and DoD Agencies.

The intent of the module is not to train experts in SwA coding and other implementation techniques but to provide the DoD acquisition workforce an awareness of SwA in the development environment and throughout the entire system lifecycle.

Course Objectives:

1. Identify the risks associated with software
2. Define Software Assurance (SwA)
3. Identify the key aspects of DoD SwA policy and guidance
4. Associate the SwA activities and their purposes and where they occur across the acquisition life cycle
5. Associate the acquisition professional or organization with their SwA responsibilities
6. Identify contractual requirements that implement SwA
7. Identify additional resources for next steps in SwA

DEPARTMENT OF DEFENSE
AGENCY

ASSURANCE OF DEPARTMENT OF DEFENSE (DoD) SYSTEMS
SECURITY CLASSIFICATION GUIDE (SCG)

Purpose

This document sets the minimum standard for classifying information about the assurance of DoD Systems, components (including hardware, firmware, and software), products, composed solutions, or systems, including vulnerabilities and weaknesses associated with DoD System, and hardware assurance (HwA) and software assurance (SwA) activities.

Applicability and Scope

If a command, program, or agency has a specific SCG whose scope includes DoD system components, that guide takes precedence over the content of this guide, as long as the command or agency guidance adheres to the minimum standard set in this guide.

JFAC/DAU/CSIAC Software Assurance Cyber Experiment (CYBEX) Workshop

Goal:

To gather a highly experienced, functionally-diverse group of practitioners, and, using current DoD guidance/documentation, walk through an exemplar to evaluate two draft acquisition guides developed by the Software Engineering Institute (SEI) and sponsored by JFAC

Materials:

- SEI DoD Program Managers Guidebook for Software Assurance
- SEI DoD Developers Guidebook for Software Assurance
- Matrix used to document results as practitioners walk through program lifecycle
- IDA developed assurance case used to structure participant findings and final report

Results:

- Produced comments and feedback for SIE DoD guidebooks
- Identified Top 10 focus areas for Software Assurance
- Published report of workshop findings and results (https://jfac.navy.mil)

Distribution Statement A: Approved for public release. Distribution is unlimited. DOPSR Case #19-S-0017

Science and Technology Portal

Producers

DARPA, DIU, IARPA, DASD(R) etc.

Needs

The ability to share work completed (in a finished or unfinished state)

The ability to be contacted for addition work on efforts in progress

The ability to review and accept new "challenges" to complete for program teams

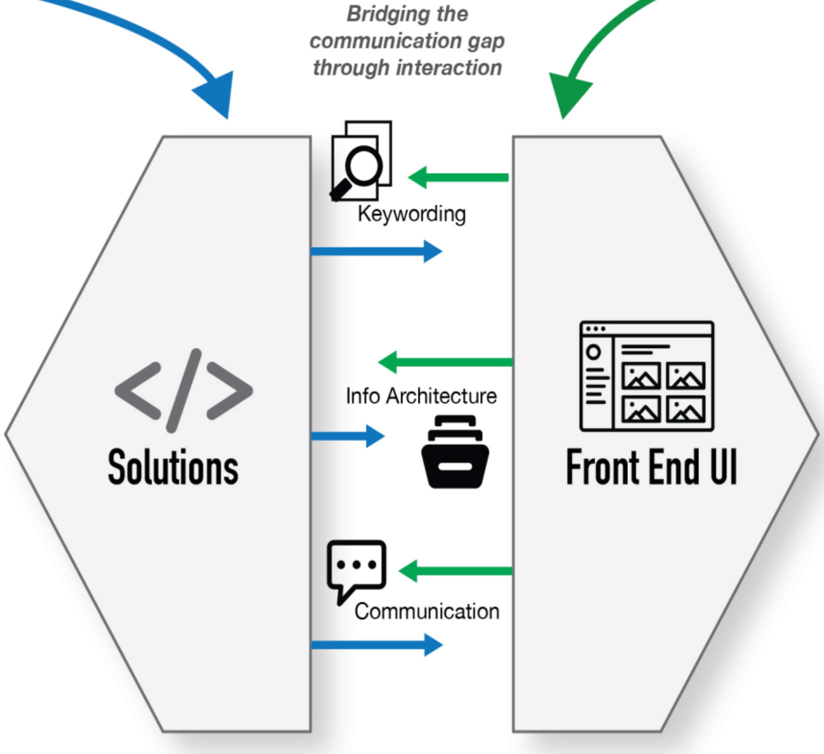
The ability to keyword content to increase the chances of proper software being found within the system

Pitfalls

Communication - Verbiage breakdown between the two groups based on the type of words they use.

Proper Keywording - Development groups identify with the intended functionality they are completing, not always the specific use (the problem)

Workload - Groups may have cycles to complete efforts but are unaware of the urgency of the effort so important efforts can go unnoticed or never be found.



5,000 DOD Programs and ORGS

Science and Technology Portal

Two distinct user groups with very different usability requirements

Consumers

DARPA, IARPA, PMOs

Needs

The ability to access work completed (in a finished or unfinished state)

The ability to contact development groups for addition work on efforts in progress

The ability to present new "challenges" to complete for program teams

The ability to search keyword content to increase the chances of proper software being found within the system

Pitfalls

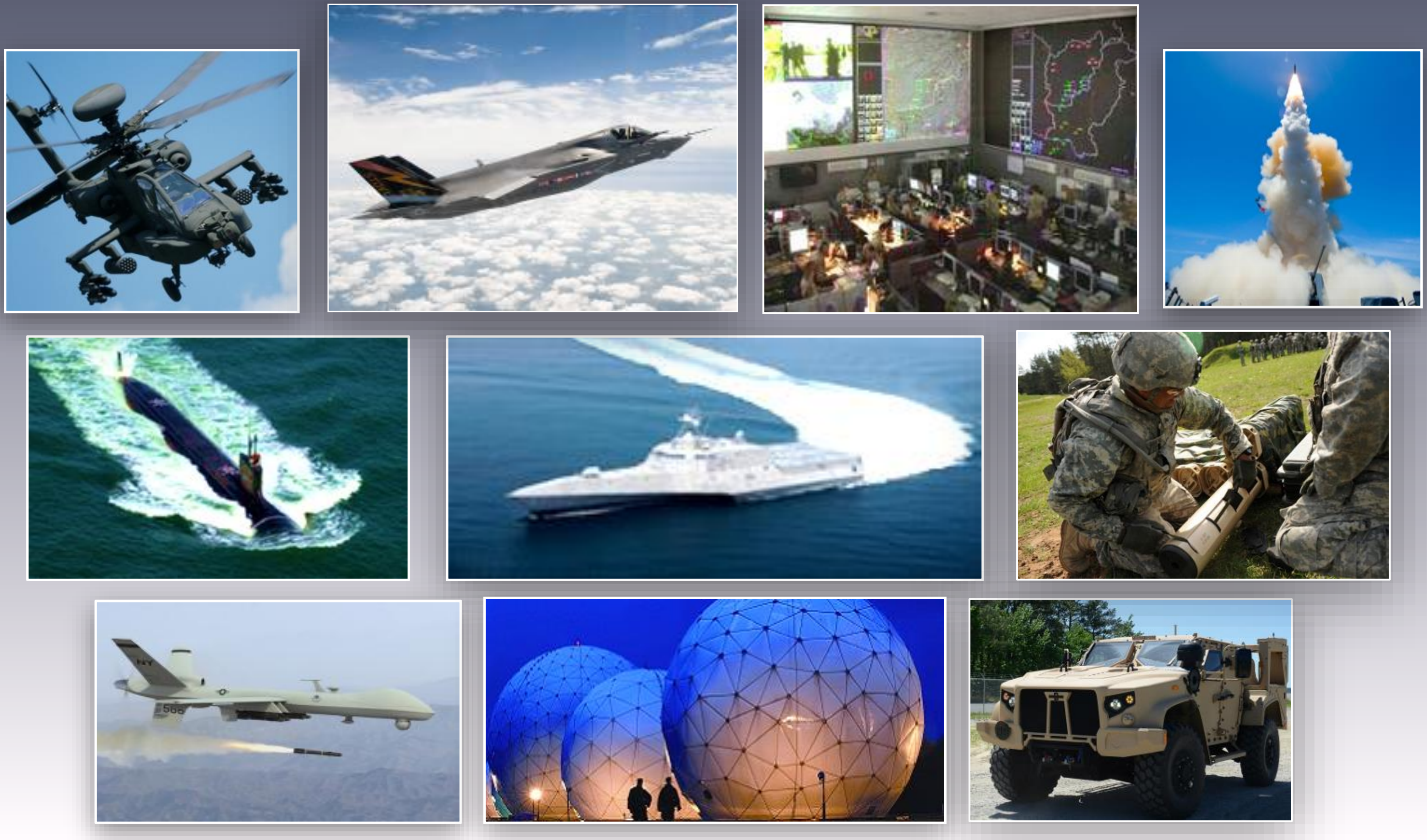
Communication - Users know what the "problem" is but not necessarily what the solution is.

Proper Keywording - The non-technical users looking for a solution may use different words to describe their needs than developers

Uncertainty - The users will often times not know what will solve their problem even if an acceptable solution is already available to them.

Distribution Statement A: Approved for public release. Distribution is unlimited. DOPSR Case #19-S-0017

DoD Research and Engineering Enterprise
Solving Problems Today – Designing Solutions for Tomorrow



For Additional Information

Mr. Thomas Hurt

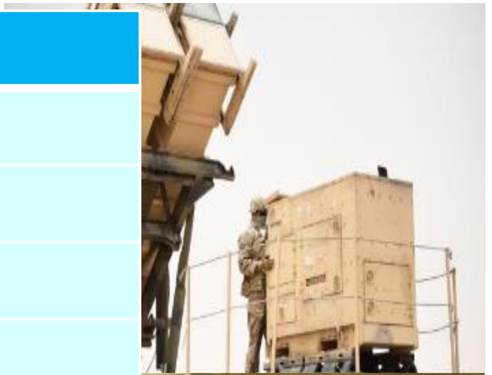
Office of the Under Secretary of Defense for Research and Engineering

571-372-6129

thomas.d.hurt.civ@mail.mil

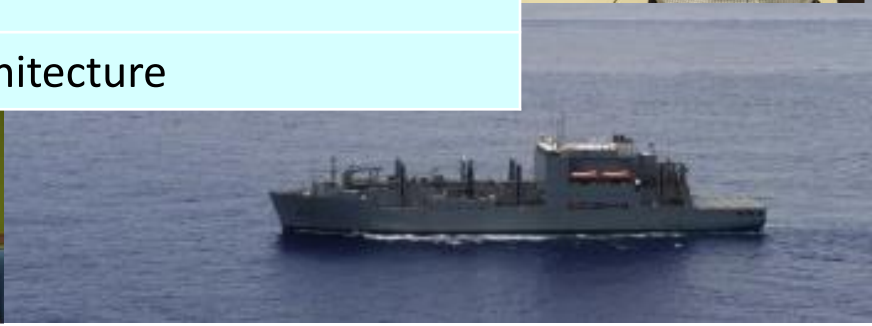
Distribution Statement A: Approved for public release. Distribution is unlimited. DOPSR Case #19-S-0017

CYBEX Top-Ten SwA Concerns



Overall Top Ten SwA Concerns

1. Evaluate of reused COTS/software
2. Integrate Agile development methods
3. Address SANS top 25 fundamental weaknesses
4. Define workforce training per role
5. Prioritize appropriate application of SwA standards
6. Integrate SwA with engineering/security efforts
7. Acquire sufficient data rights
8. Use performance-based, standard metrics
9. Adopt a risk-based approach
10. Plan for future threats and architecture



Distribution Statement A: Approved for public release. Distribution is unlimited. DOPSR Case #19-S-0017

CYBEX Top-Ten Guidebook Suggestions

Carnegie Mellon University
Software Engineering Institute

DRAFT

Program Manager's Guidebook for Software Assurance

Dr. Kenneth E. Nidiffer
Dr. Carol Woody
Timothy A. Chick

August 2018

SPECIAL REPORT
CMU/SEI-2018-SR-025

Software Solutions and CERT Divisions
[Distribution Statement C] U.S. Government Agencies and their contractors only.

http://www.sei.cmu.edu

Top Ten Guidebook Suggestions
1. Organize by processes as well as by acquisition phases
2. Address data rights across life-cycle
3. Highlight code version control tracking practices
4. Expand SwA guidance for post-Critical Design Review (CDR)
5. Address FPGA/ASIC/firmware development
6. Integrate Mission-Based Cyber Risk Assessment (MBCRA) to prioritize SwA activities
7. Normalize SwA risk into overall systems scoring method
8. Describe SwA impacts on other system functional areas such as reliability, survivability, safety, maintainability, & performance
9. Relate Agile processes with traditional phases/milestones
10. Provide guidance on Sw development infrastructure management to reduce SwA technical debt

Carnegie Mellon University
Software Engineering Institute

DRAFT

DoD Developer's Guidebook for Software Assurance

Dr. William R. Nichols, Jr.
Dr. Thomas Scanlon

August 2018

SPECIAL REPORT
CMU/SEI-2018-SR-013

Software Solutions and CERT Divisions
[Distribution Statement C] U.S. Government Agencies and their contractors only.

Distribution Statement A: Approved for public release. Distribution is unlimited. DOPSR Case #19-S-0017