



DoD Joint Federated Assurance Center (JFAC) Industry Outreach

Thomas D. Hurt

Office of the Deputy Assistant Secretary of Defense
for Systems Engineering

Timothy A. Chick

CERT | Software Engineering Institute

Paul R. Croll

Co-Chair, NDIA Software Committee

Dr. Kenneth E. Nidiffer

Software Engineering Institute

19th Annual NDIA Systems Engineering Conference
Springfield, VA | October 26, 2016



JFAC Mission

The JFAC is a federation of DoD organizations that have a shared interest in promoting software and hardware assurance in defense acquisition programs, systems, and supporting activities. The JFAC member organizations and their technical service providers interact with program offices and other interested parties to provide software and hardware assurance expertise and support, to include vulnerability assessment, detection, analysis, and remediation services, and information about emerging threats and capabilities, software and hardware assessment tools and services, and best practices.





SwA Tool Enterprise Licensing Initiative



- **Problem:**
 - Application of software assurance tools and techniques across DoD is inconsistent -- and often after engineering and development are completed, when few resources are available for remediation
 - Expertise of best practices is isolated in various programs
 - Cost of SwA tools and lack of general knowledge about how to properly use them hampers widespread adoption
 - Use of SwA tools is not optimized for remediation of vulnerabilities by engineers
- **Solution: Break down barriers to wider adoption of SwA tools and practices throughout DoD**
 - Provide enterprise-wide licenses for SwA tools to promote better and wider use
 - Provide training and expertise to engineers and developers for how and when to best use SwA tools
 - Simplify acquisition of SwA tools by systems and SW engineers by moving from thousands of individual program and organization acquisitions across DoD to 1 per vendor
 - Simplify use of SwA tools by providing one centralized automated ticket-based request and download mechanism available throughout DoD, including direct support contractors
- **Status: Piloting programs => Transitioning to enterprise solutions**



Current SwA Tool Acquisition Process



- **Word-of-mouth and vendor recommendation**
- **Hundreds (perhaps thousands) of individual transactions across disparate DoD programs and organizations**
- **Sometimes acquired from GSA schedule, with a small discount (or not)**
- **Separate licenses may be needed for every software developer, including contractors, with no sharing or dynamic allocation**
- **Potential tool users include 50,000+ DoD programs, centers, test organizations, cyber ranges, blue and red teams, ...**
- **Cost for mainstream programs is full price licenses and thousands of concurrent acquisitions, program-by-program**
- **Additionally, programs**
 - May buy maintenance, but more likely to use old tools
 - May not realize the lead time involved in planning for tool procurements
 - May not be aware of various potential solutions, including freeware



SwA ELA Pilot Project Process

- **Initial SwA tool requirements were determined by Services using JFAC Software Technical Working Group and DoD-wide SwA tool use data call**
- **Services established priority for enterprise license buys**
- **Services established policy and guidance for programs to use JFAC-provided licenses, not ad hoc purchase**
- **USACE conducted the acquisition of SwA tools**
- **JFAC portal automated license management**
 - License allocation, tracking, and inventory management
 - Pilot program demonstrated proof of concept for centralized license distribution
- **Next step: demonstration of dynamic license allocation to maximize use of vulnerability detection tools throughout DoD**

The most effective and efficient cyber strategy is to eliminate detectable vulnerabilities and weaknesses in software while it is being engineered and developed, not after it has been breached.



Lessons Learned from Pilot

- Pilot project was able to demonstrate proof of concept for investing in enterprise licensing agreements (ELAs) for SwA tools and technologies.
- Program offices seemed to accept to idea that this initiative could help them save money, reduce program risks, and result in much better software for their programs.
- The pilot showed an ELA can be managed effectively by a small number of people, and with minimum investments in additional infrastructure and technology.
- SwA tool vendors seemed more than willing to work with us because it gave them greater access to DoD system software developers and assessors, and minimized the overhead costs of doing multiple negotiations with individual programs.
- There are major efficiencies and savings to be gained for both the government and the vendor in doing bulk buys and centralized management of commonly needed SwA tools and services.



JFAC Software Assurance (SwA) Enterprise Licensing Pilot Lessons Learned

Timothy A. Chick
CERT | Software Engineering Institute

19th Annual NDIA Systems Engineering Conference
Springfield, VA | October 26, 2016



Disclaimers



- **Copyright 2016 Carnegie Mellon University**
- **This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.**
- **Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.**
- **NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.**
- **[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.**
- **This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.**
- **Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.**
- **DM-0004010**



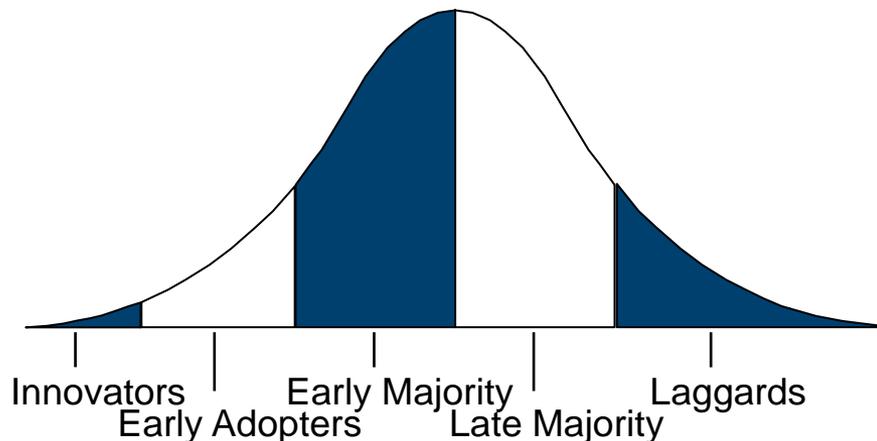
JFAC Software Assurance



- **Objective:** Improve the assurance of software deployed and operated throughout the DoD
- **Function:** Identifies, promotes, and facilitates access to software assurance (SwA) tools and best practices in support of the DoD.
- Liaison for interagency efforts to improve SwA throughout the US Government
 - Create a focal point for DoD services to share expertise and best practices
 - Ensuring an inventory of SwA resources across DoD
 - Increase awareness of and access to:
 - Software assurance tools, across the software lifecycle
 - Evidence-based practices
 - Support environments
 - Expertise regarding SwA competencies, threats, and vulnerabilities



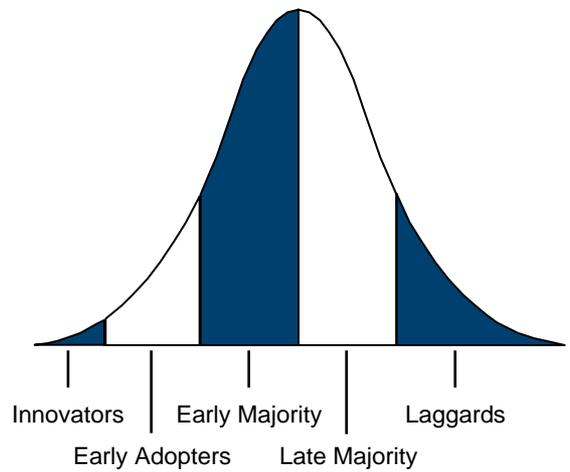
SwA Tools and Techniques Adoption Issues



- **Analyzing software to identify and remove weaknesses is a critical program protection countermeasure.** Unfortunately, it can be difficult to determine what types of tools and techniques exist for analyzing software, and where their use is appropriate.
- A **potential advantage of tools is scalability**; manual approaches can be too costly or time-consuming for large software systems.
- SwA tools are expensive and many programs either cannot afford them, do not understand their value, or do not understand how to use them. Thus are **resisting the adoption** and the DoD is not consistently using them across the enterprise.

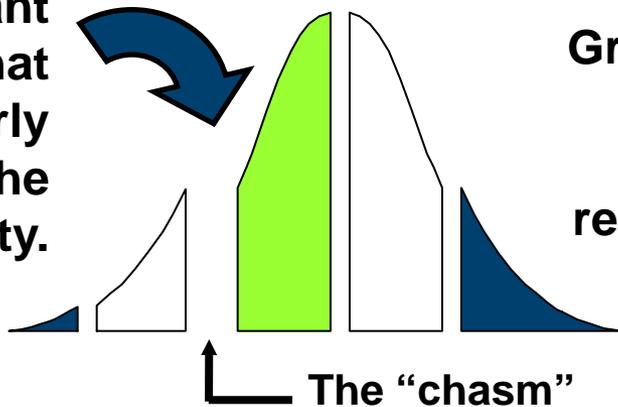


Overcoming SwA Adoption Issues



- The use of SwA tools within the DoD is still in the early adoption phase.
- JFAC Enterprise Licensing is focused on providing the infrastructure needed to jump the chasm within the DoD.
- While issuing SwA licenses to the early adopters, JFAC has simultaneously focused on building the needed infrastructure to begin crossing the chasm.

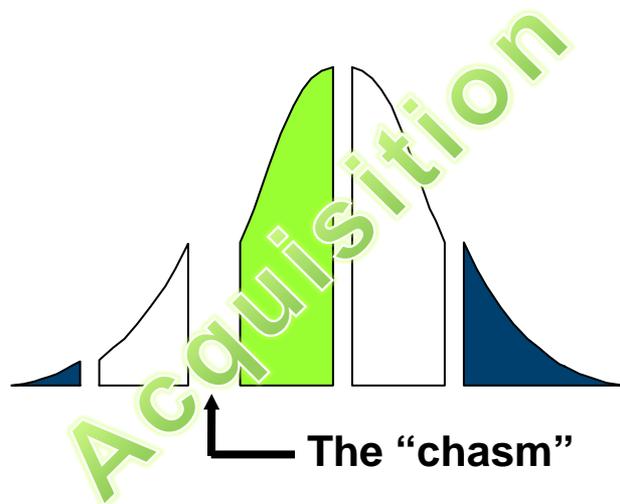
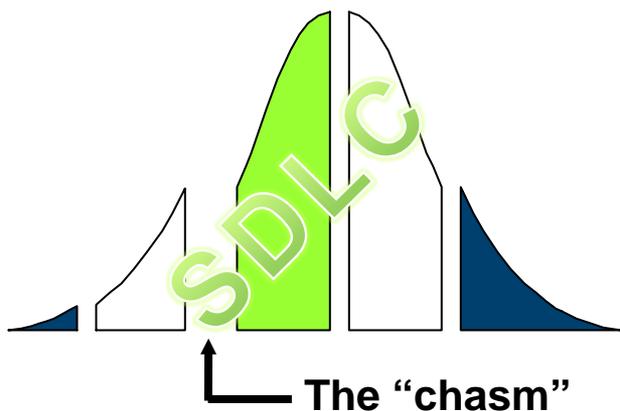
The most significant gap is the one that separates the early adopters from the early majority.



Groups to the right of early adopter also need positive references from early adopters.



Two Chasms to Cross



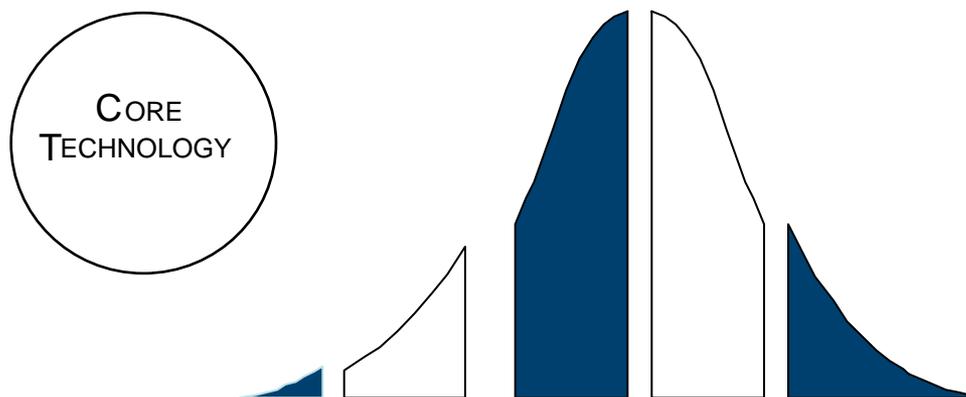
- This pilot is focused on solving the SDLC chasm
- We need to address the Policy/PEO/PMO chasm too
- The experience and knowledge gained from addressing the SDLC chasm will help inform the later.
- **Acquisition**
 - Policy changes on acquisition requirements
 - DAU knowledge and training
 - Contract language guidance
 - PM training for oversight
 - DoD enablement of contractors
 - DoD SDLC SwA models / body of knowledge



Innovators and Early Adopters Can Adopt SwA Tools and Integrate Them into Their SDLC on Their Own



- **When a technology is first introduced, the focus is on the “thing” itself . . . the core technology.**
- **In this case the core technology is the Software Assurance Tools themselves.**



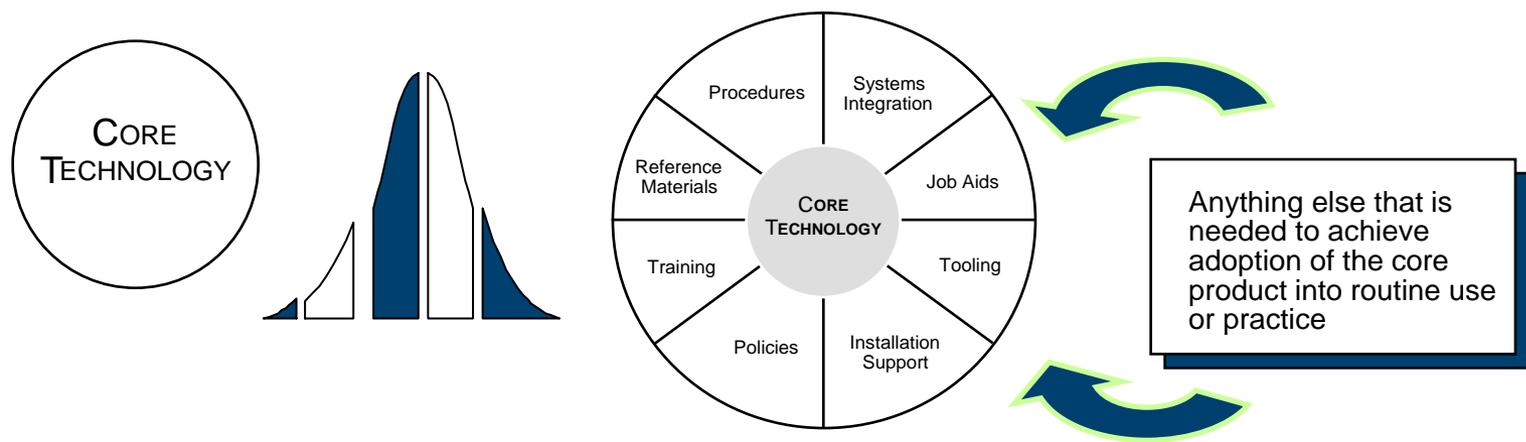
Individuals least in need of support are the technology enthusiasts.
These people can cobble together bits and pieces of systems and build their own rough whole product.



Bridging the Gap for the DoD Mainstream



For the majority of adopters, the technology must be augmented by an integrated suite of services and ancillary products to become the “whole product.”



As part of the pilot JFAC has focused on various elements of change in order to improve DoD adoption of SwA tools and techniques.



Getting DoD to Adopt SwA Tools



In order to jump the chasm, JFAC has begun

- Creating **awareness** of why SwA Tools need to be used
- Building **desire** to support and use the SwA tools being provided
- Providing the **knowledge** needed to install and start using the SwA tools
- Demonstrate **ability** of programs to find and fix vulnerabilities using SwA tools
- Provide **reinforcing** environment to sustain SwA tool adoption and use



Creating Awareness and Desire



The Department Representatives have used the “Free Tools” available through the pilot to increase awareness and desire to participate, by removing the cost barrier.

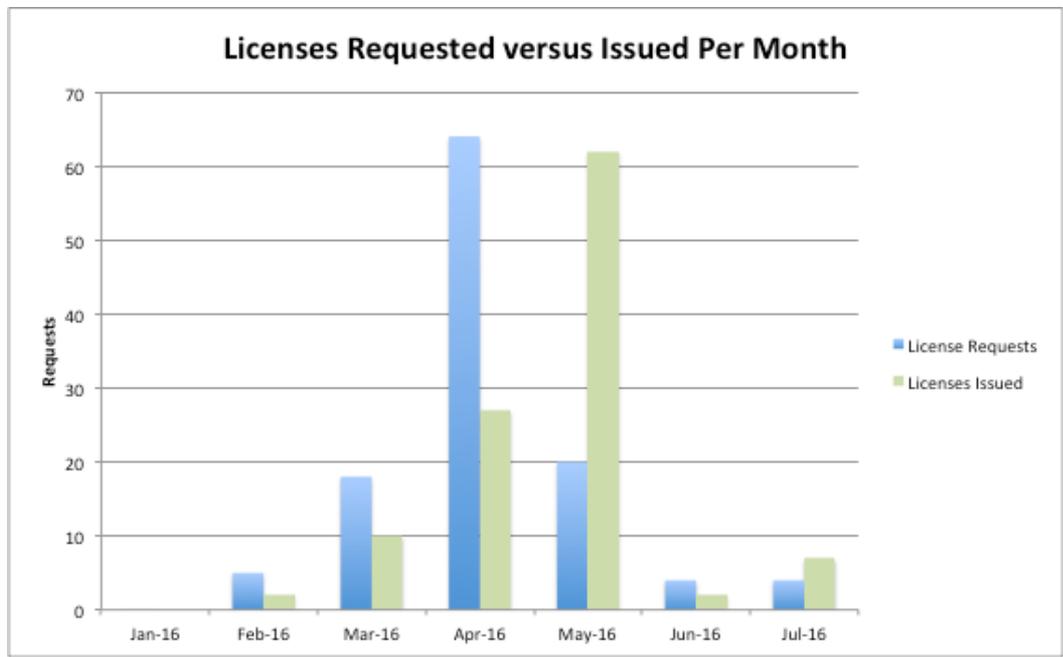
JFAC has also worked on communicating how the SwA tools enable compliance with DoD Guidance:

- Deputy Assistant Secretary of Defense – Systems Engineering, Program Protection Plan Outline & Guidance. [DASD(SE) 2011]
- DoD Instruction 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN) [DoDI 5200.44]
- Defense Acquisition Guidebook (DAG), Ch 13
- Section 933 of Public law 112-239-Jan. 2, 2013



Lessons Learned from Pilot

- It can take months of messaging in order to get projects to “volunteer” or agree to use SwA tools
- While the licenses were available as early as October 2015, request for their use did not begin until February 2016





Knowledge



- **JFAC Resources:**

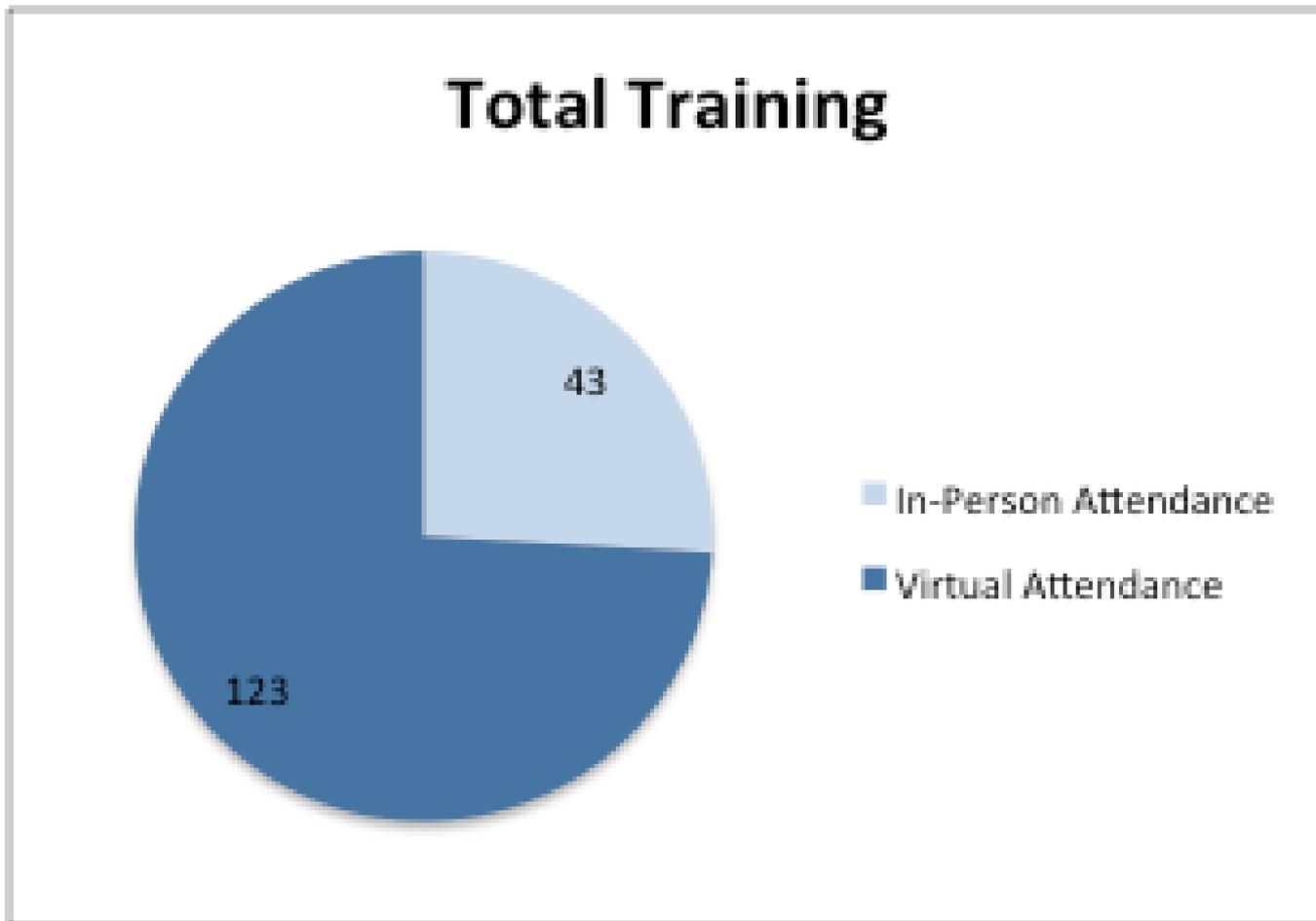
- JFAC-CC <https://jfac.army.mil>
- JFAC Collaboration Portal <https://intelshare.intelink.gov/sites/jfac/>

- **Tool Training**

- All training included an option of in-person or virtual participation and the training was recorded as a training resource to be added to the JFAC Portal.
- During the pilot phase JFAC sponsored tool training for 5 tools



Training Participation





Lessons Learned from Pilot



- Websites were not available until after the pilots were started. This led to:
 - Confusion as to where to go to request licenses
 - Difficulty in tracking and reporting on licenses issued
 - A lack of resources for pilots to understand what tools were actually available to them
 - No basic training on the available tools and how to use them
- Licenses availability was less than expected, thus Department Representatives had to deny license requests after previously promising licenses.
- Video production can take months to complete, thus videos are not available immediately after training event.
- Coordinating dates and time for vendor training needs to occur months in advanced of actual training event.
- Participation of training was lower than desired due to limited advanced advertising and limited distribution lists.



Ability



- The pilot survey is not scheduled to go out until the end of September, thus we do not have overall summary feedback from pilot participants.
- Lessons Learned from Pilot
 - Ability to obtain approval to install SwA tools on various pilot program networks was extremely constrained due to network policies. Thus limiting the pilot's ability to use the tool to find and fix vulnerabilities.
 - The use of AMRDEC SAFE for distributing SwA applications is insufficient due to slow upload and file size limitations



Reinforcing Environment



- **Moving beyond the pilot and investing in DoD Enterprise Licenses is the next step in expanding DoD adoption of SwA tools and techniques.**
- **In addition to providing the needed licenses, JFAC will continue to work on improving SwA tool support infrastructure based on the lessons learned from the pilot.**



NDIA Systems Engineering Division (SED) Software Committee

Dr. Kenneth E. Nidiffer
Software Engineering Institute

19th Annual NDIA Systems Engineering Conference
Springfield, VA | October 26, 2016



Charter



- **DASD/SE* requested the NDIA SED Software Committee to provide an industry perspective regarding opportunities for “DASD/SE to improve the practice of software engineering”**
 - **The Software Committee held several virtual meetings and identified eleven areas for consideration**
 - **These areas were then ranked in terms of Payoff and Ease of Implementation**
 - **Detailed recommendations were developed for seven opportunities for improvement**
- *DASD/SE = Deputy Under Secretary of Defense for Systems Engineering



Recommendations for Software Initiatives



1. **Agile/Incremental Software Development**
2. **Improved Software Estimation and Integration with EVM and Technical Metrics**
3. **Test Optimization**
4. **Model Based System Development**
5. **Requirements Quality (Systems and Software)**
6. **DoD 5000 Lifecycles: Incorporation of High-Impact Software Enabling Technologies**
7. **Software Assurance in Acquisition, Development, and Sustainment**

Next Step: Develop a strategy to provide a software assurance framework for benchmarking industry



Committee Members

- Paul Croll, PR Croll LLC (Chair)
- JoAn Ferguson, General Dynamics
- Gary Hafen, Lockheed Martin (retired);
- Cheryl McIntyre, Lockheed Martin
- Cynthia Molin, Raytheon
- Ken Nidiffer (Co-Chair), SEI
- Shawn Rahmani, Boeing
- Rick Selby, Northrop Grumman
- Tim Walden, Lockheed Martin



Summary

- **We are working with industry to address needs for better SwA tools and technologies**
 - SwA Tool License Pilot Program demonstrated efficiencies to be gained by centrally managing and distributing tools and licenses through a JFAC portal maintained by the JFAC Coordination Center.
- **We are working with industry to advance the state of practice for SwA within DoD**
 - NDIA SE Division re-assembled its software experts group and engaged in an exploration of SwA capabilities, gaps and potential solutions.
- **How You Can Help:**
 - We need industry input and participation in developing improved tools and technologies
 - Some identified needs include making tools more widely available during software architecting, design, development, and testing; lowering the cost of tool acquisition for programs; and workforce training
 - Continue to partner with us to advance knowledge and management of assurance tools, techniques and training

Support programs with SW, HW and FW assurance



For Additional Information



Thomas D. Hurt
Deputy Director, Software
Assurance and Software
Engineering, DASD(SE)
571-372-6129 |
thomas.d.hurt.civ@mail.mil

Timothy Chick
CERT | Software Engineering
Institute
Carnegie Mellon University
412-268-1473
tchick@cert.org

Paul R. Croll
Co-Chair, NDIA Software Committee
PR Croll LLC
540-903-6497 |
pcroll@computer.org

Dr. Kenneth E. Nidiffer
Director of Strategic Plans for
Government Programs,
Carnegie Mellon University
Software Engineering Institute
703-247-1387 |
nidiffer@sei.cmu.edu



Systems Engineering: Critical to Defense Acquisition



Defense Innovation Marketplace
<http://www.defenseinnovationmarketplace.mil>

DASD, Systems Engineering
<http://www.acq.osd.mil/se>