NDIA Workshop Report: DoD and Defense Industry Analysis of DoD Software Assurance (SwA) Capability Gaps

June 22-23 2017

Holly Dunlap
Raytheon
NDIA SSE Committee Chair
Holly.Dunlap@Raytheon.com

Dr. Kenneth E. Nidiffer
Director of Strategic Plans for Government Programs
Carnegie Mellon University
Software Engineering Institute
Email (SEI): nidiffer@sei.cmu.edu
Email (OSD): kenneth.e.nidiffer.ctr@mail.mil

NDIA* Workshop Sponsors

This event was a jointly sponsored workshop by **NDIA SED, NDIA SSE & SwA Committees** with the DoD's **Joint Federated Assurance Center (JFAC) SwA Community of Practice (CoP),** hosted by **MITRE,** with analysis provided by **Engility Corporation**.

*NDIA – National Defense Industrial Association

Overview

- **Workshop Purpose & Participants**
- **Background**
- **Workshop Activities**
- **Analysis and Observations**

Workshop Purpose

- The government conducted a DoD Software Assurance (SwA) Capability Gap Analysis and afforded the defense industry an opportunity to review and provide their perspective.

- The workshop participants – from industry and gov't – provided a diverse set of background experiences, and allowed for a better consideration of different perspectives.

- This workshop provided insight into what industry believes are SwA gaps and priorities that affect U.S. technical capability advantage.

Workshop Participants

33 participants from industry and government

- **CACI**
- **Engility Corp**
- **General Dynamics**
- **IDA**
- **Lockheed Martin**
- **MITRE**
- **Northrup Grumman**
- **Raytheon**
- **SEI**
- **DASD(SE)**
- **DoD CIO**
- **DOE**
- **Army**
- **Navy**
- **Air Force**

Report developed by Dr. Scott Brown and Ms. Madison Rudy (Engility Corporation) in coordination with NDIA leads and Mr. Tom Hurt, DASD(SE).

Background

In July 2016, the JFAC SwA Technical Working Group identified **63 DoD capability gaps** that prevent the effective planning and execution of software assurance within the DoD acquisition process. The gaps were organized into seven categories:

1) Life cycle planning and execution
2) SwA technology
3) Policy, guidance, and processes
4) Resources
5) Contracting and Legal
6) Metrics
7) Federated Coordination

As chair of the JFAC Steering Committee, Ms. Kristen Baldwin, Acting Deputy Assistant Secretary of Defense for Systems Engineer (DASD(SE)), approved the analysis and directed the Technical Working Group to **develop a strategy to address the identified gaps**.

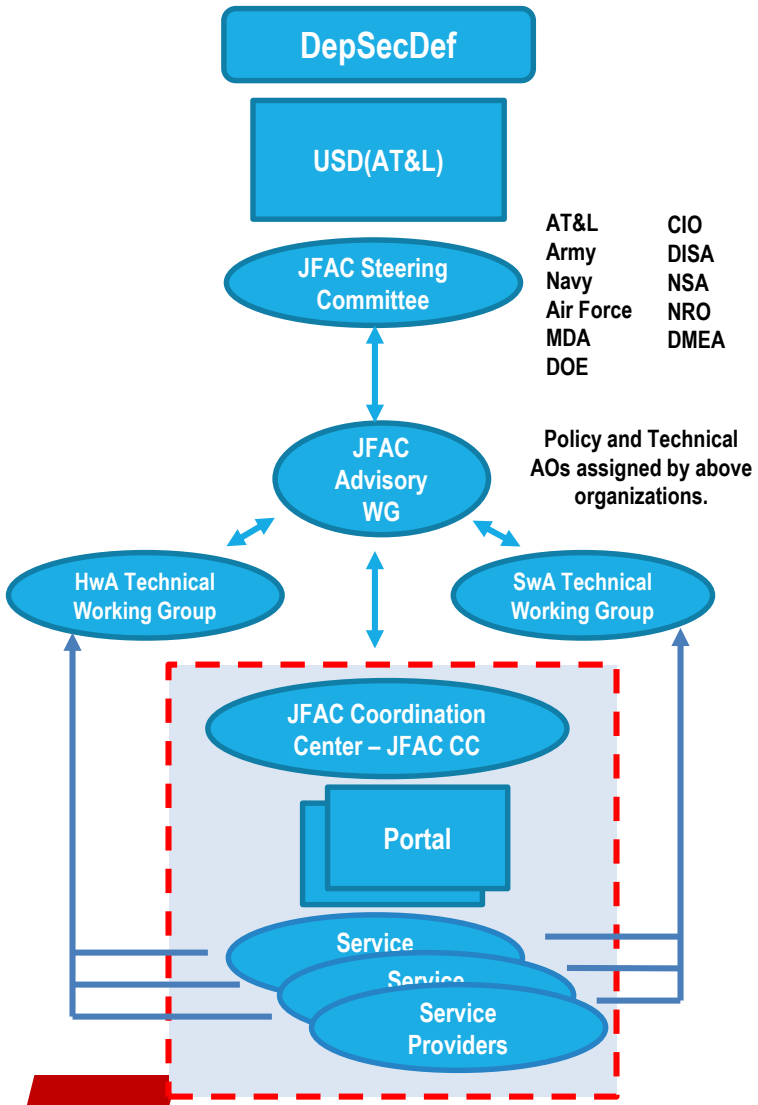
DASD(SE)'s JFAC lead, Mr. Tom Hurt, agreed to support an **NDIA-sponsored joint industry-government workshop**.

Background – FY14 NDAA Section 937

- **Key provisions:**
  - "provide for the establishment of a **joint federation of capabilities** to support the trusted defense system needs…to ensure security in the **software** and **hardware** developed, acquired, maintained, and used by the Department"
  - "consider whether capabilities can be met by existing centers"
  - **"[if gaps] shall devise a strategy [for] resources [to fill such gaps]"**
  - "[NLT 180 days, SECDEF shall] issue a **charter**…"
  - "submit to congressional defense committees…a **report** on funding and management"
- **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
  - R&D program to improve code vulnerability analysis and testing tools
  - Requirements to procure manage, and distribute enterprise licenses for analysis tools

DoD established the Joint Federated Assurance Center in 2014; JFAC reached IOC in 2016.

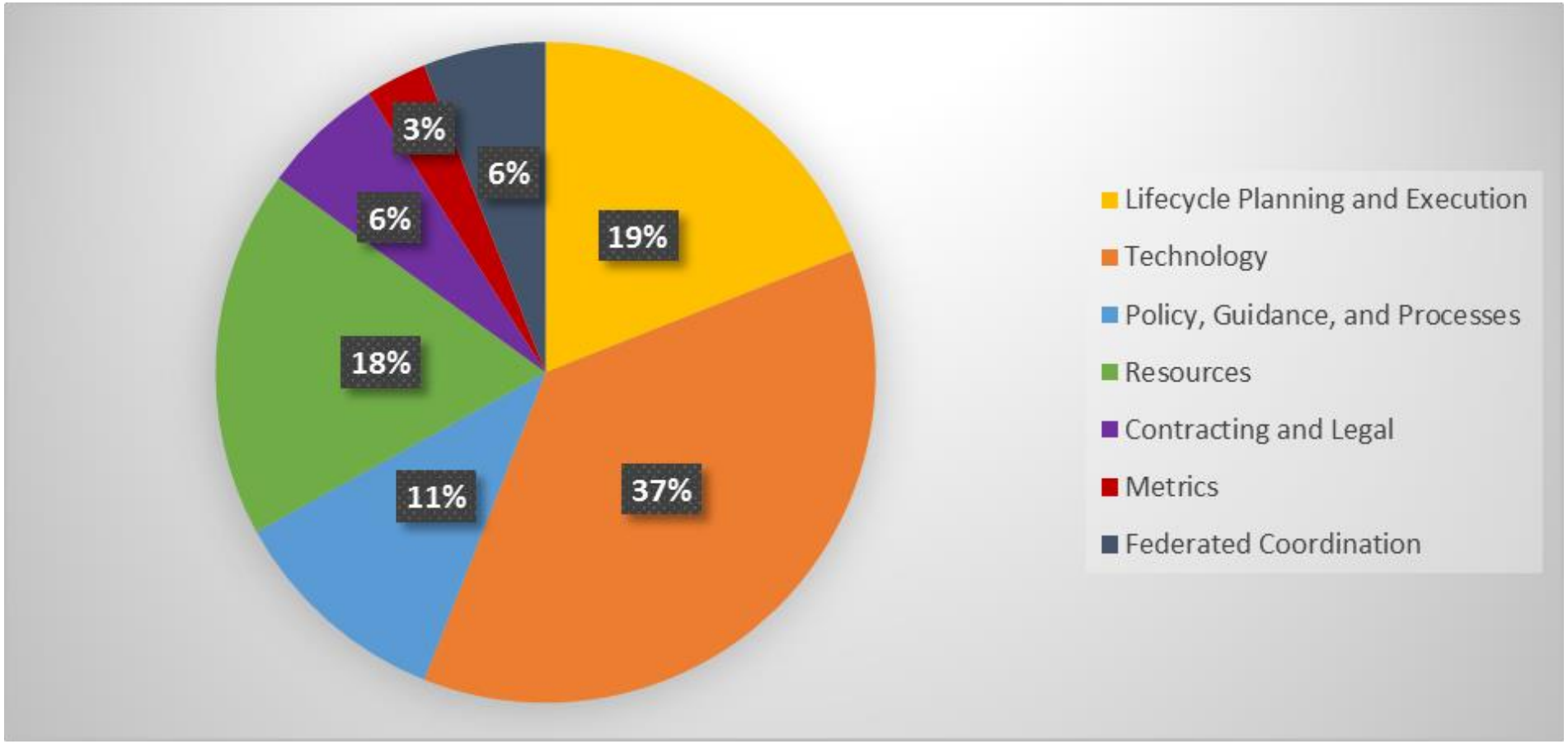
Background – JFAC Operational Structure



- **JFAC Action Officer (AO) WG**
  - AOs for SES-level JFAC Steering Committee
  - Maintain enterprise and strategy cognizance
  - Reporting and ROI status
- **SwA and HwA Working Groups**
  - Collaboration and shared prioritization in daily/weekly activities, meet on a regular basis
  - Provide policy guidance
  - Provide community focal point for “hard problem” analysis and question/answer
- **JFAC Coordination Center**
  - Coordination of **Service Providers**
  - Supports programs with situational awareness, information/best practices, coordination
  - SwA analysis tool license distribution
  - **Portal:** https://jfac.army.mil
  - Assessment Knowledge Base (future)

Background – JFAC SwA Technical Working Group Capability Gap Analysis

Gaps (63 total) were categorized into seven areas*



*This graphic is from the JFAC SwA Technical Working Group Capability Gap Analysis Report (Distribution C, available from DASD(SE)).

Six Sigma Voice of the Customer (VOC)

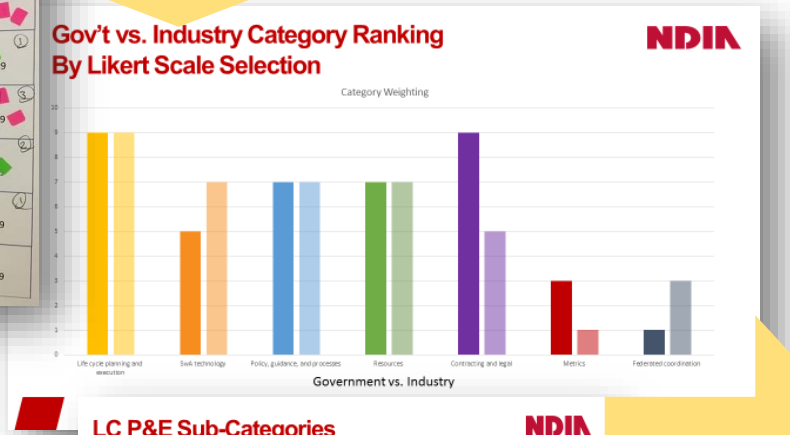
- The “voice of the customer” is a process used to **capture the requirements/feedback from the customer (internal or external)** to provide the customers with the best in class service/product quality. This process is all about being **proactive and constantly innovative to capture the changing requirements of the customers** with time.
- The “voice of the customer” is the term used to describe the **stated and unstated needs or requirements of the customer.** The voice of the customer can be captured in a variety of ways: Direct discussion or interviews, surveys, focus groups, customer specifications, observation, warranty data, field reports, complaint logs, etc.
- This data is used to **identify the quality attributes needed** for a service provider to incorporate in the process or product.

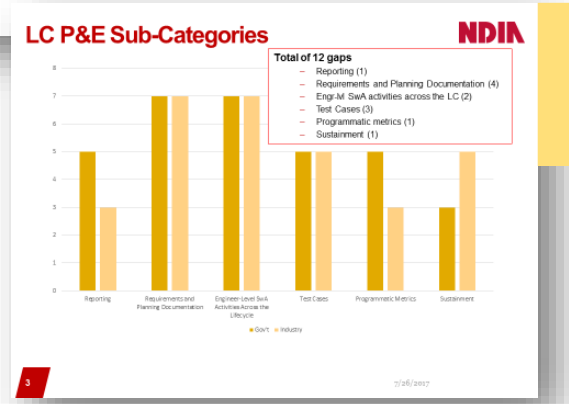
Workshop Activities

JFAC SwA Capability Gap Analysis

Government	Industry

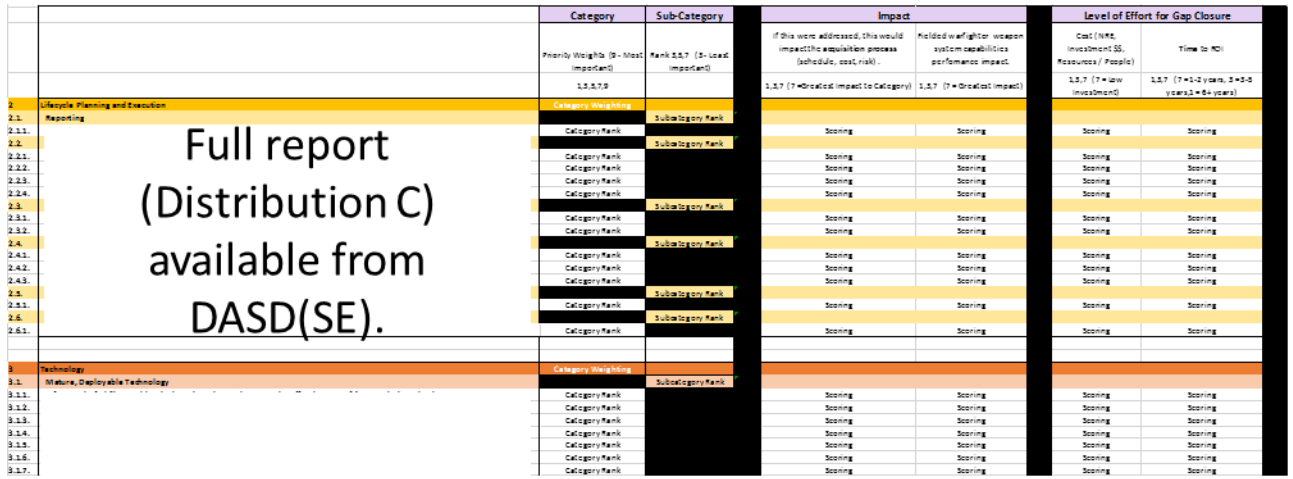
Prioritized Gap Categories & Sub-categories





Voice of the Customer (VOC) Assessment

Government	Industry



Facilitated Break-out Sessions (Combined gov't/industry)	Assess (Individually)
1. Lifecycle planning & execution 2. SwA technology 3. Policy, guidance, process and Federated Communication 4. Resource 5. Contracts, Legal and SwA metrics	<u>Influence</u> • Acquisition (cost, schedule, risk) • Weapon system capability <u>Level of effort</u> to close gap • Cost • Time to ROI

SwA Capability Gap Analysis
"Voice of the Customer" Worksheet

63 SwA Gaps

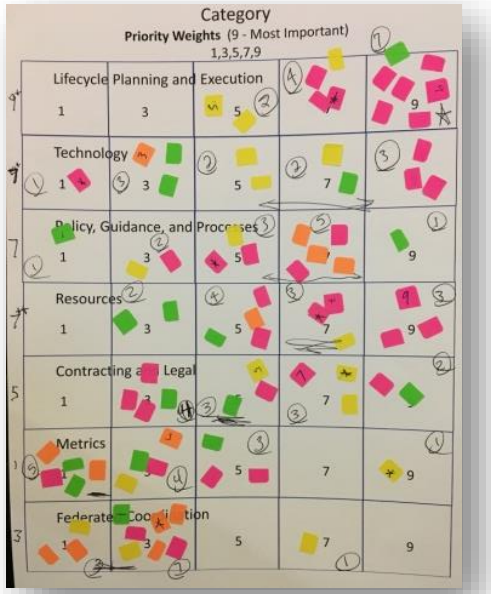
Prioritize Categories

Assess Influence/Level of Effort

		Category	Sub-Category	Influence		Level of Effort for Gap Closure	
		Priority Weights (9 - Most Important)	Rank 3,5,7 (3 - Least Important)	If this were addressed, this would impact the **acquisition process** (schedule, cost, risk) .	Fielded warfighter weapon system capabilities perfomance impact.	Cost (NRE, Investment $$, Resources / People)	**Time** to ROI
		1,3,5,7,9		3,5,7 (7=Greatest influence)	3,5,7	3,5,7 (7=lowest cost)	3,5,7 (7=1-2 yrs, 5=3-5 yrs, 3=5+ yrs)
2	Lifecycle Planning and Execution	Category Weighting					
2.1.	Reporting		Subcategory Rank				
2.1.1.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.2.			Subcategory Rank				
2.2.1.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.2.2.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.2.3.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.2.4.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.3.			Subcategory Rank				
2.3.1.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.3.2.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.4.			Subcategory Rank				
2.4.1.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.4.2.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.4.3.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.5.			Subcategory Rank				
2.5.1.		Category Rank		Scoring	Scoring	Scoring	Scoring
2.6.			Subcategory Rank				
2.6.1.		Category Rank		Scoring	Scoring	Scoring	Scoring
3	Technology	Category Weighting					
3.1.	Mature, Deployable Technology		Subcategory Rank				
3.1.1.		Category Rank		Scoring	Scoring	Scoring	Scoring
3.1.2.		Category Rank		Scoring	Scoring	Scoring	Scoring
3.1.3.		Category Rank		Scoring	Scoring	Scoring	Scoring
3.1.4.		Category Rank		Scoring	Scoring	Scoring	Scoring
3.1.5.		Category Rank		Scoring	Scoring	Scoring	Scoring
3.1.6.		Category Rank		Scoring	Scoring	Scoring	Scoring
3.1.7.		Category Rank		Scoring	Scoring	Scoring	Scoring

Full report (Distribution C) available from DASD(SE).

Group Sessions – Category / Sub-category Analysis



- **During a facilitated session, participants were divided by Government and Industry affiliation to score the seven gap categories and their respective sub-categories.**

- **Each participant was provided voting 'chits' – one for each gap and sub-category – and was asked to score each category / sub-category using a Likert scale (1-9, where 9 = highest priority):**

- **The two groups discussed their voting to seek understanding of individual scores and an agreed to rank.**
  - A groups' averaged score based on individual votes was calculated to compare / contrast between Government and Industry.

Gap Category Ranking By Likert Score & Mean Value

The table below provides the ranked categories by each groups' averaged Likert scores and rank.

Rank	Category (Government Likert average & rank)	Category (Industry Likert average & rank)
1	Contracting and Legal (7.18 / 9)	Lifecycle Planning and Execution (7.77 / 9)
2	Lifecycle Planning and Execution (7 / 9)	Resources (6.17 / 7)
3	Policy, Guidance and Processes (5.89 / 7)	Technology (5.55 / 7)
4	Resources (5.45 / 7)	Policy, Guidance and Processes (5.5 / 7)
5	Technology (5.18 / 5)	Contracting and Legal (5.5 / 5)
6	Metrics (3.91 / 3)	Metrics (3.15 / 1)
7	Federated Coordination (2.6 / 1)	Federated Coordination (2.82 / 3)

* Where two categories received the same average value, rank numbers are interchangeable.

Observations – Gap Categories and Sub-categories

- **Lower ranking does not denote lack of importance of the category / sub-category or the associated gaps.**
  - Participants were required to use all Likert scale values – something had to be a 1.
  - Each and every one of the 63 gaps has one or more Government organization 'sponsors'.
- **Contracting and Legal category had largest difference in Likert rank and score.**
  - Government felt strongly that without explicit contractual direction, contractors' SwA activities would not be sufficient; Industry recognized the priority and importance of contract language, but as engineers participating in the workshop, they focused on engineering-focused categories.
  - Individual gap scores in this category did rank in the top quartile (see slide 17)
- **The only sub-category with more than 1 Likert rank difference was Policy.**
- **Metrics and Federated Coordination were ranked lowest because participants felt the Government had started to address the associated gaps.**
  - Industry gave the lowest Likert score to Metrics although the actual votes averaged 3.15, higher than Federated Coordination (score: 2.82).
  - JFAC has produced some (initial) metrics for JFAC web portal and SwA tool use.
  - JFAC has a several working groups and communities of practice in addition to a web portal that allows for coordination. Biggest need: ability to include industry in coordination / collaboration

Breakout Session – Gap Analysis

- **During facilitated break-out sessions for each of the gap categories, groups consisting of both Government and Industry participants discussed the gaps in their assigned category.**
- **After discussion, each individual participant was asked to score each category gap using a Likert scale (3-5-7) in the VOC worksheet, assuming the gap could be closed:**
  - Influence: how would gap closure positively influence acquisition cost/schedule/risk (e.g., lower acquisition cost) and warfighter capability (e.g., 7 = highest influence of capability)
  - Level of Effort: how much cost (e.g., 7 = lowest cost to close gap in terms of funds or resources) and how long before time to Return of Investment for gap closure (e.g., 3 = 6 or more years)
- **VOC worksheets were collected and analyzed after the workshop concluded.**
  - Weighted scores were calculated with and without category/sub-category scores.

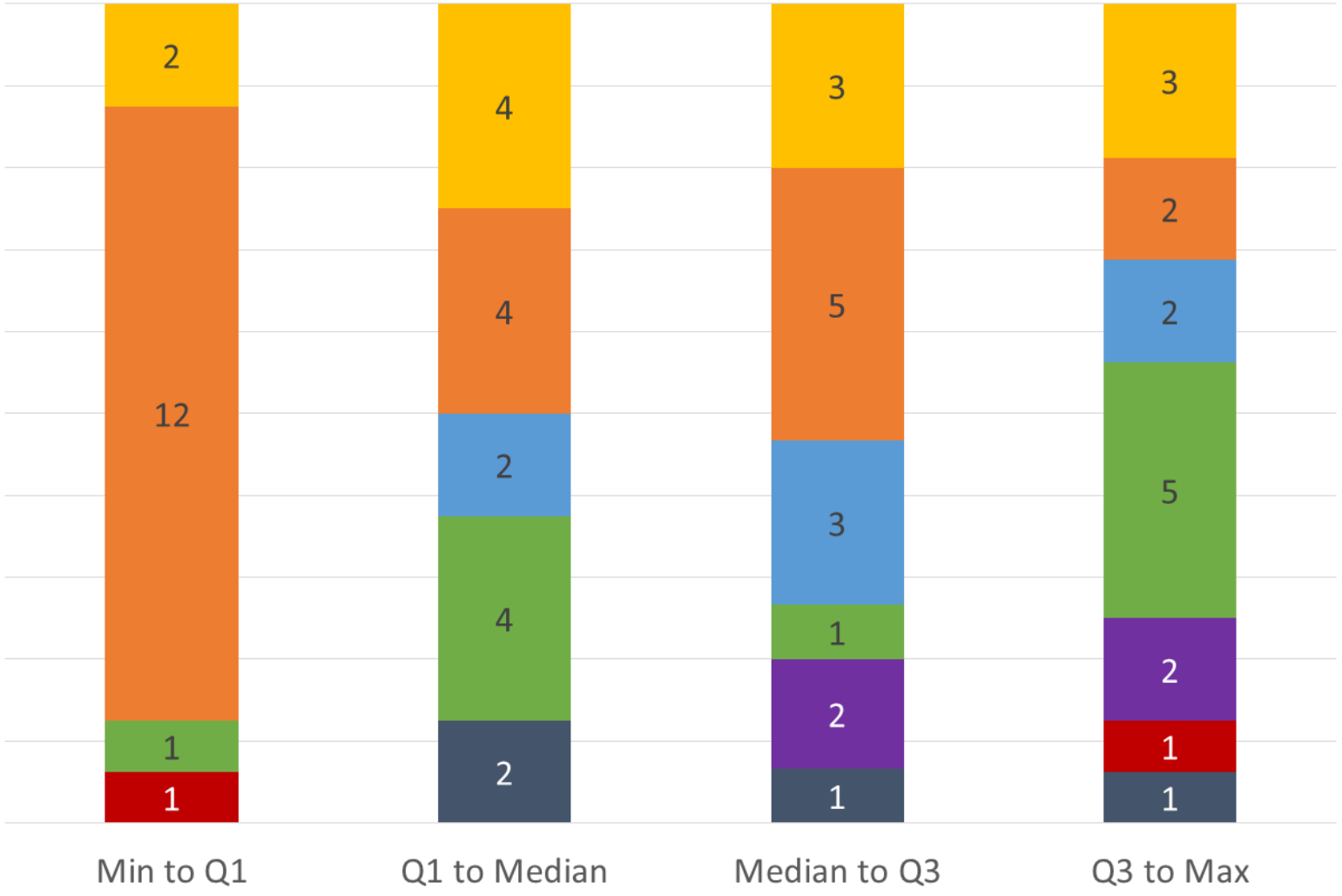
VOC Gap Analysis – Gaps in Top Quartile by Weighted Score

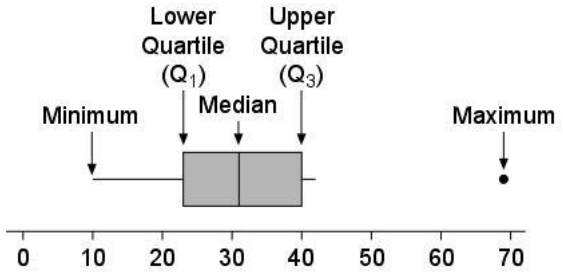
Weighted Gap Score = Influence(acquisition process) * Influence score(warfighter capability) * LOE(cost) * LOE(time to ROI)

1	Contracting and Legal	6.1 - Lack of definitive contract language for SwA planning and execution activities, as early in the lifecycle as possible
2	Resources	5.2.1 - Lack of SwA training for Program Managers
3	Resources	Tools
4	Metrics	7.1 - Lack of agreed-upon metric set that will be collected and analyzed
5	Policy, Guidance and Processes	Policy
6	Federated Coordination	8.4 - Lack of enterprise-wide approval for tool use on networks
7	Technology	3.1.4 - Lack of use of defense technology
8	Lifecycle Planning & Execution	2.2.2 - SwA requirements lacking in system requirements
9	Resources	Training
10	Technology	Deployable Technology
11	Resources	Tools
12	Resources	Tools
13	Policy, Guidance and Processes	Process
14	Lifecycle Planning & Execution	SwA Activities
15	Contracting and Legal	6.2 - Lack of strategy for SwA of COTS and NDI
16	Lifecycle Planning & Execution	2.1.1 - No clear reporting requirement on software assurance planning, activities, and status

Full report (Distribution C) available from DASD(SE).

Number of Gaps by Category per Quartile based on Weighted Gap Scores





Observations – VOC analysis

- **All categories have 1 or more gaps in the highest quartile based on Influence/Level of Effort scores**
  - This analysis validates the keynotes, group and break-out discussions at the workshop – even if a gap was in a low ranked category (e.g., Metrics), the associated gaps may have high “pay-off” (i.e., ability to reduce program cost/schedule/risk and improve warfighter capabilities, low cost/resources to implement and quick time to ROI)
- **Each category, except Technology, has at least half of its gaps in the top 50%; Contracting & Legal has all its gaps in top 50%.**
  - Technology gaps, composing the largest number of gaps (37%), had some of the lowest Time to ROI scores
  - The highest scored gap was in Contracting & Legal – “Lack of definitive contract language for SwA planning and execution activities, as early in the lifecycle as possible”

Observations – "Missing" Gaps

- **Life Cycle Planning and Execution**
  - SwA needs to flow into industry documents as well (SW Dev Plan) (Gaps 2.2.1 & 2.2.2)
  - Lack of operator's perspective in life cycle (Gap 2.3)
- **Technology**
  - Lack of integrated build environment with Software Assurance tools
  - Lack of ability to select appropriate technologies based on program characteristics
- **Policy & Guidance / Federated Coordination**
  - Unification – relationship mapping and coordination of statute, policies and guidance. U.S. Code; DFARS; DoDI 5000.02, 8500; NIST, …. They are pointing to each other.
  - Coverage – Policy & Guidance needs to cover whole life cycle, all technologies, all systems regardless of ACAT level or type (e.g., weapon system vs. IT)
  - Industry access to JFAC & associated capabilities (e.g., Assessment Knowledge Base)

Observations – "Missing" Gaps

- **Resources**
  - Industry expertise is also a gap.
  - Specialized SwA workforce is NOT the answer. System and SW engineers need to understand SwA.
  - SwA training is not available across DoD career fields or restricted to certain career fields
  - Software Engineering Body of Knowledge has not been adopted across the DoD in terms of minimum skill sets (such as the IEEE SWEBOK)
- **Contracts / Metrics**
  - Need consistency between all security related areas in what is put in contract language
  - Legality of doing analysis of the COTS software before you buy it
  - Legality of publishing results of doing analysis of the COTS software (make the DeWitt clause illegal)
  - Providing incentives for robust vendor software assurance program
  - Research into improved metrics – for projects

Conclusion and Way Forward

- **This workshop served to provided insight into what industry believes are SwA gaps and priorities that affect U.S. technical capability advantage.**

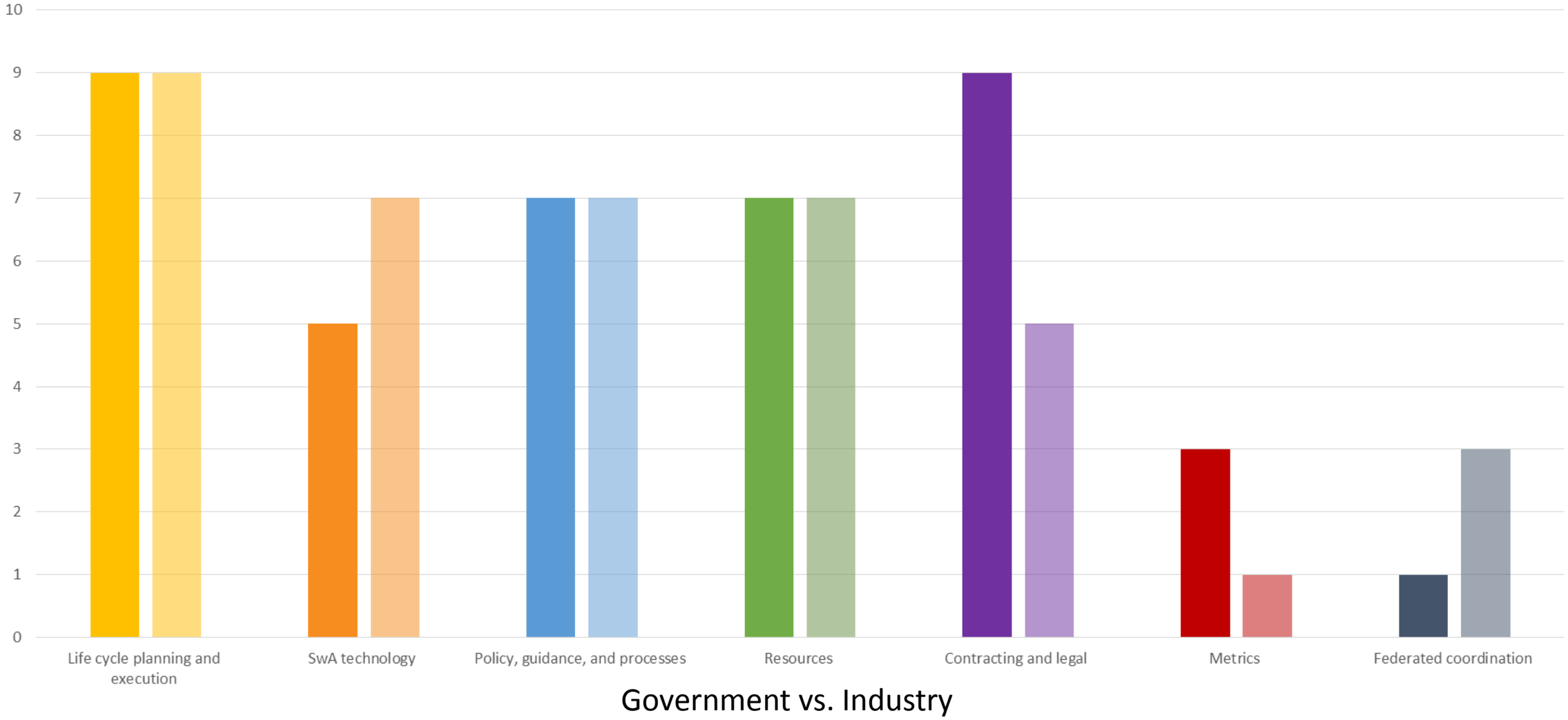
- **The analysis quantifies and validates ongoing discussion in JFAC working groups and other DoD and NDIA venues (e.g., Cyber Resilient Weapon System workshops) – there is high payoff expected if we address Software Assurance gaps.**

- **Analysis will be presented at various forums.**
  - NDIA SE Fall Conference: Holly Dunlap & Tom Hurt

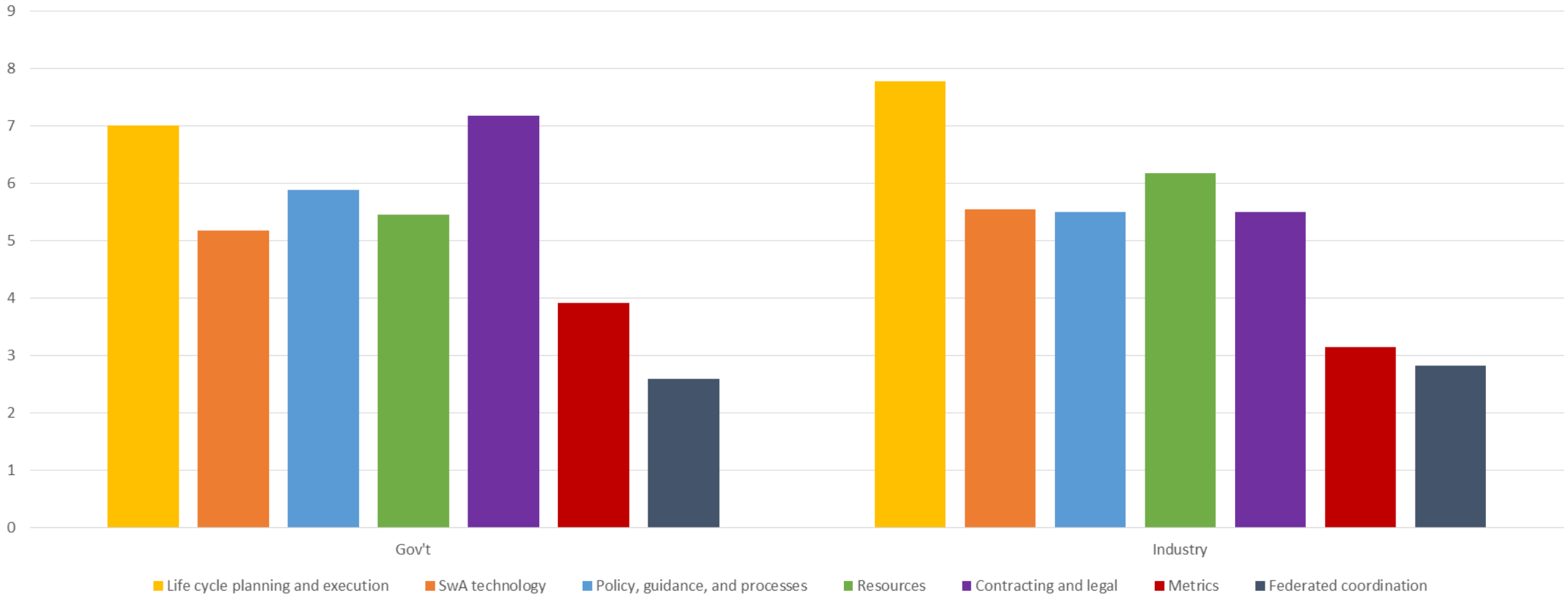
- **“High payoff” initiatives will be considered for funding based on analysis.**

Supporting Material

Gov’t vs. Industry Category Ranking By Likert Scale Selection



Gov’t vs. Industry Groups’ Averaged Likert Score



Government vs. Industry

Category Ranking By Likert Scale Selection

- **The following table provides the group selected category ranking grouped by Government and Industry.**
- **Where two categories are given the same Likert scale value, rank numbers for that group are interchangeable.**

Rank	Government Category	Industry Category
1	Lifecycle Planning and Execution (9)	Lifecycle Planning and Execution (9)
2	Contracting and Legal (9)	Technology (7)
3	Policy, Guidance, and Processes (7)	Policy, Guidance, and Processes (7)
4	Resources (7)	Resources (7)
5	Technology (5)	Contracting and Legal (5)
6	Metrics (3)	Federated Coordination (3)
7	Federated Coordination (1)	Metrics (1)