Improving Systems Engineering through Operational Risk Management

Brian Gallagher
SVP, Operational Excellence
CACI, Inc.

Dr. Ken Nidiffer
Dir. of Strategic Plans for Government Programs
Carnegie Mellon University
Software Engineering Institute

Software Engineering Institute

CACI
EVER VIGILANT

Problem Statement

- **Many programs fail to address the real operational need when fielding new capabilities resulting in a gap between business and mission needs and operational capabilities.**
- **Two major root causes**
  - Requirements failed to capture true mission and business needs
  - The mission and business needs evolve during development and project team fails to evolve as quickly
- **Gaps between need and capability increases operational risk.**

Example: ECSS Air Force

- Expeditionary Combat Support System (ECSS) began development in 2004
- Program had vague set of objectives
- Lack of clarity in operational need and what mission and business needs were being addressed
- Major disconnect between solving critical operational threats and risks versus solving strategic needs (cost reduction, affordability, consolidation, etc.)
- Result: $1.1B in wasted funding and a system that was not deployable

"The Air Force's Expeditionary Combat Support System, or ECSS., is a prime example of how a system designed to save money can actually waste billions of taxpayer dollars without producing any usable capability." – Sen. John McCain

Example: Improvised Explosive Device (IED) Defeat

- **During Operation Iraqi Freedom, IEDs posed a new and real threat**
  - Existing capabilities couldn't detect or defeat the threat
  - The military urgently needed new capabilities fast
- **Army created the Joint IED Defeat Organization (JIEDDO) with the sole purpose of defeating this new operational risk**
  - Ability to bypass traditional acquisition process
  - Fielded less mature, but effective solutions
  - Lives were saved
- **Quickly fielded systems lacked certain quality attributes such as robustness, evolvability, and maintainability**
- **Tactical mission risks mitigated yet strategic business risks ignored: Total Cost of Ownership and Logistical Complexity Increased**

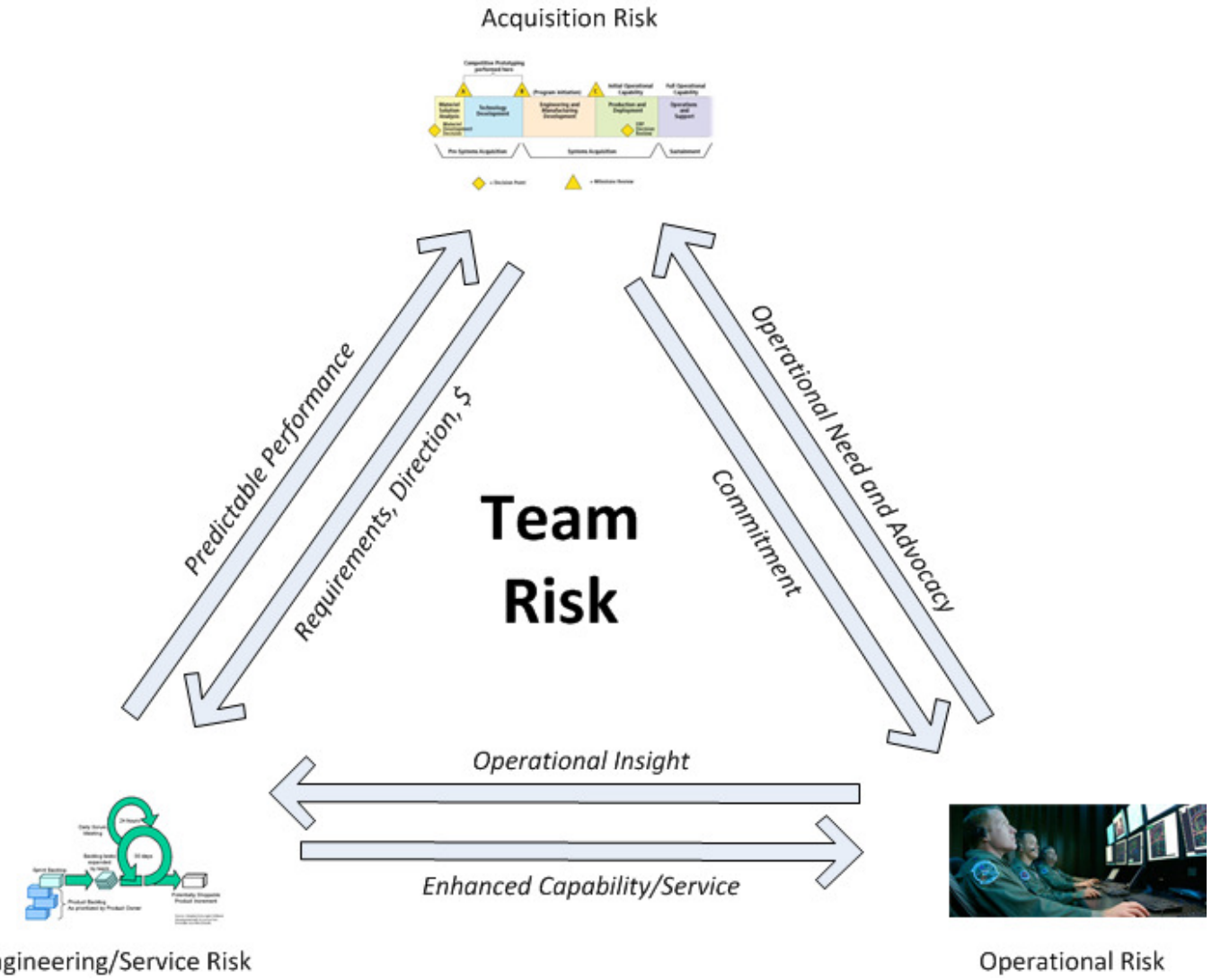
Operational Risk to Balance the Need

- The purpose of any new system, component or capability development should be to mitigate operational risk
- During development, operational risk changes
- Systems engineering activities during the project lifecycle should evolve through operational risk considerations

Typical Risk Management

- **Acquisition Risk Management During Acquisition Planning and Execution**
  - Focus is on programmatic risk
- **Program and Engineering Risk Management During Development**
  - Identify and mitigate risks associated with cost and schedule
  - Identify and mitigate technical risks associated with technical approach
- **Concept of Operational Risk is Lacking**

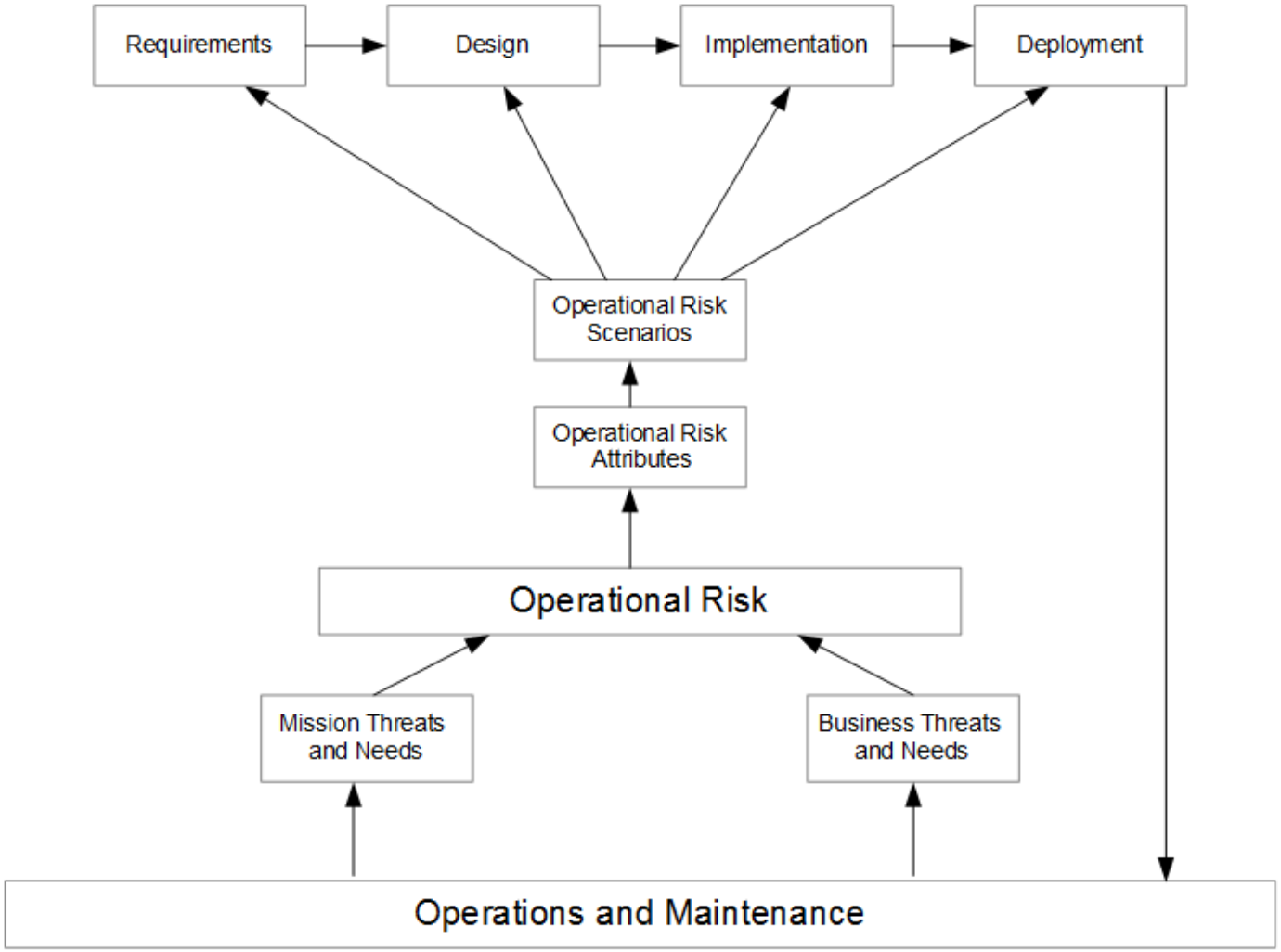
The More Effective Approach



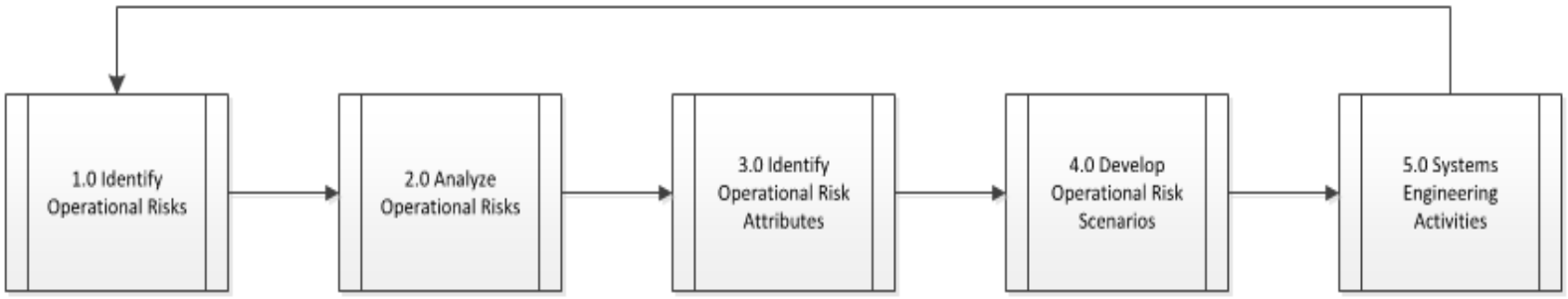
Software Engineering Institute

CACI
EVER VIGILANT

Operational Risk-Driven Engineering Requirements/ Engineering Development (ORDERED)



ORDERED Steps



CACI
EVER VIGILANT

ORDERED Risk Taxonomy

ORDERED Taxonomy			
A. MISSION		B. BUSINESS	
1. Mission Planning		1. Resource Planning	
	a. Stability		a. Workforce
	b. Completeness		b. Budget
	c. Clarity		c. Facilities
	d. Feasibility		d. Organizational Structure
	e. Precedence		
	f. Agility		
2. Mission Execution		2. Governance	
	a. Effeciency		a. Policies
	b. Effectiveness		b. Procedures
	c. Repeatability		c. Facilities
	d. Agility		d. Contracts
	e. Affordability		e. Analytics
	f. Security		f. Compliance
	g. Safety		g. Risk Management
3. Mission Outcomes		3. Strategic Planning	
	a. Predictability		a. Vision and Mission
	b. Accuracy		b. Values
	c. Usability		c. Goals
	d. Timely		d. Objectives
	e. Efficient		e. Monitoring
4. Operational Systems		4. Stakeholder Management	
	a. Throughput		a. Identification
	b. Usability		b. Stakeholder Mgmt Plan
	c. Flexibility		c. Engagement
	d. Reliability		d. Controlling
	e. Evolvability		
	e. Security		
	f. Supportability		
	f. Inventory		
5. Operational Processes		5. Culture	
	a. Suitability		a. Integrity
	b. Repeatability		b. Values
	c. Predictability		c. Norms
	d. Agility		d. Rewards
	e. Security		
6. Operators		6. Continuous Improvement	
	a. Skill Level		a. Problem Identification
	b. Training		b. Opportunity Identification
	c. Turnover		c. Root Cause Analysis
	d. Affordability		d. Improvement Planning
			e. Implementation

Example: Cyber Security Operations Center*

- **The purpose of the CSOC is to ensure that cybersecurity incidents do not impact agency operations.**

Mission Objectives	Business Objectives
1. Detect, contain, and remediate cyber security threats. 2. Analyze trends, determine root causes, and improve system resilience. 3. Educate system operators and maintainers on cybersecurity threats.	1. Reduce cybersecurity related incidents. 2. Reduce cost of cybersecurity activities. 3. Position for agency organizational consolidation.

*Case study is fictitious and any resemblance to a real program or agency is not intended

Example: CSOC – Identify Operational Risks

- **Risks identified by operational users during a facilitated workshop using the ORDERED taxonomy**

Risk ID	Risk Statement
CSOC001	Incident occurance is unpredictable; may not have adequate resources to respond during crisis
CSOC002	Heavy compliance and oversight make processes rigid; may not be able to adjust quickly to new events
CSOC003	Current intrusion detection system is proprietary and vendor is not responsive when changes are needed; system may not detect newer threats, cost of support is high
CSOC004	We hire new operators with little experience; Lower mission effectiveness
CSOC005	80% of operator time is spent responding to incidents; may not see trends or understand root cause of indidents

Example: CSOC – Analyze Operational Risks

- **Risks characterized by probability and impact and sorted into "Top 5"**

Top "N"	Risk ID	Risk Statement	Prob	Imp	Risk Exposure
1	CSOC004	We hire new operators with little experience; Lower mission effectiveness	4	4	16
2	CSOC003	Current intrusion detection system is proprietary and vendor is not responsive when changes are needed; system may not detect newer threats, cost of support is high	4	4	16
3	CSOC005	80% of operator time is spent responding to incidents; may not see trends or understand root cause of indidents	4	2	8
4	CSOC001	Incident occurance is unpredictable; may not have adequate resources to respond during crisis	4	2	8
5	CSOC002	Heavy compliance and oversight make processes rigid; may not be able to adjust quickly to new events	2	3	6

Example: CSOC – Identify Risk Attributes

- **Most important risks further clarified by identifying the attribute and attribute concern.**
  - Risk Attribute: *a characteristic of the operational mission or business which will be judged negatively by stakeholders unless the operational risk is mitigated*

Top "N"	Risk ID	Risk Statement	Risk Attributes	Attribute Concern
1	CSOC004	We hire new operators with little experience; Lower mission effectiveness	1. Operator: Training, Skill Level 2. Mission Execution: Effectiveness	Assimilation of new staff and planned growth in mission
2	CSOC003	Current intrusion detection system is proprietary and vendor is not responsive when changes are needed; system may not detect newer threats, cost of support is high	1. Operational Systems: Flexibility 2. Mission Execution: Affordability	Mission expansion and attack sophistication

Example: CSOC – Develop Risk Scenarios

- Scenarios are simply expressions of real-world interactions
- Used in engineering to express ***expected*** behavior of systems, components or capabilities
- *Operational Risk Scenarios* describe the ***unwanted*** behavior of the system that would cause mission or business impact to the operational organization.

Example: CSOC – Develop Risk Scenarios

- **CSOC Risks and Risk Scenarios**

Top "N"	Risk ID	Risk Statement	Risk Attributes	Attribute Concern
1	CSOC004	We hire new operators with little experience; Lower mission effectiveness	1. Operator: Training, Skill Level 2. Mission Execution: Effectiveness	Assimilation of new staff and planned growth in mission
	Operational Risk Scenarios 1. New operator joins organization and fails to be completely certified and capable within 2 weeks 2. OPs staff grows by 200% increasing number of teams performing the mission. New teams not fully capable of supporting operations within 1 month			
2	CSOC003	Current intrusion detection system is proprietary and vendor is not responsive when changes are needed; system may not detect newer threats, cost of support is high	1. Operational Systems: Flexibility 2. Mission Execution: Affordability	Mission expansion and attack sophistication
	Operational Risk Scenarios 1. New mission tasking requires additional intrusion detection across new agency locations. Current system fails to scale and vendor is unresponsive in making required system changes 2. A new hacker group uses alternative means to access closed system and uses technology not detected by current system. Complete re-design of detection system required to implement new detection algorithms.			

Example: CSOC – Prioritizing Risk Scenarios

Mission or Business Criticality	
HIGH	Serious mission or business impact
MEDIUM	Moderate mission or business impact
LOW	Low mission or business impact
Plan Gap	
HIGH	No accommodation based on current operations or engineering plan (requirements, design, implementation, testing, deployment)
MEDIUM	Some accommodation based on current operations or engineering plan (requirements, design, implementation, testing, deployment)
LOW	Accommodated in current operations or engineering plan (requirements, design, implementation, testing, deployment)

Example: CSOC – Prioritized Risk Scenarios

- **Based on inputs from operational staff**

Scenario Number	Operational Risk Scenario	Criticality	Gap
CSOC003-1	New mission tasking requires additional intrusion detection across new agency locations. Current system fails to scale and vendor is unresponsive in making required system changes	HIGH	HIGH
CSOC004-2	OPs staff grows by 200% increasing number of teams performing the mission. New teams not fully capable of supporting operations within 1 month	HIGH	MEDIUM
CSOC003-2	A new hacker group uses alternative means to access closed system and uses technology not detected by current system. Complete re-design of detection system required to implement new detection algorithms.	MEDIUM	HIGH
CSOC004-1	New operator joins organization and fails to be completely certified and capable within 2 weeks	MEDIUM	MEDIUM

Influencing the Engineering Process

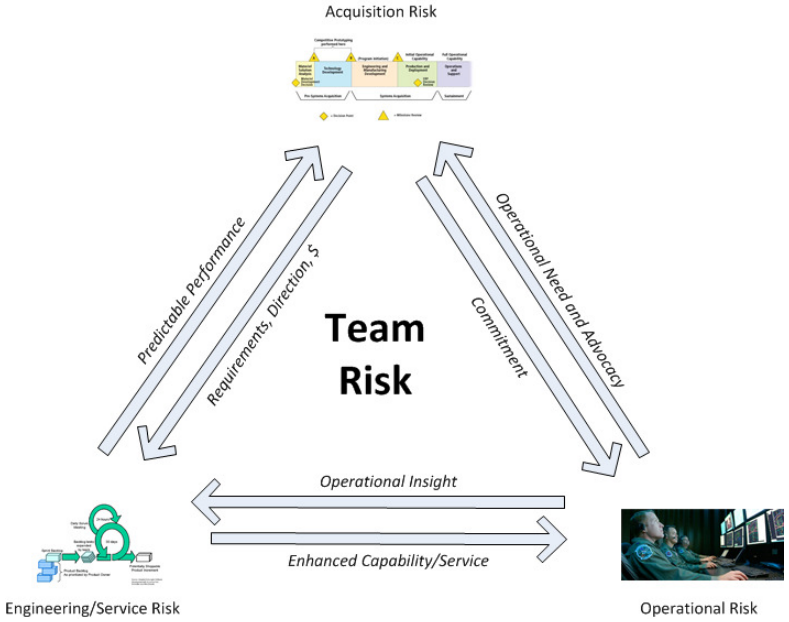
- **Continuous operational risk identification and risk scenario evolution used to influence every aspect of the systems engineering process**

Example: CSOC – Influencing the Engineering Process

- **Potential activities identified:**
  - CSOC003-1: Non-functional requirements of scalability, flexibility and evolvability were ignored. ECP issued to add additional architectural trade-studies with the goal of maximizing the non-functional requirements.
  - CSOC004-2: Lack of a separate training environment identified. Change request initiated to add the requirement for an operationally relevant training environment.
  - CSOC003-1: The architecture team had failed to consider structural and behavioral patterns that would help avoid the risk scenario. Team revised their approach and selected additional architectural patterns to increase the scalability, flexibility and evolvability of the solution.

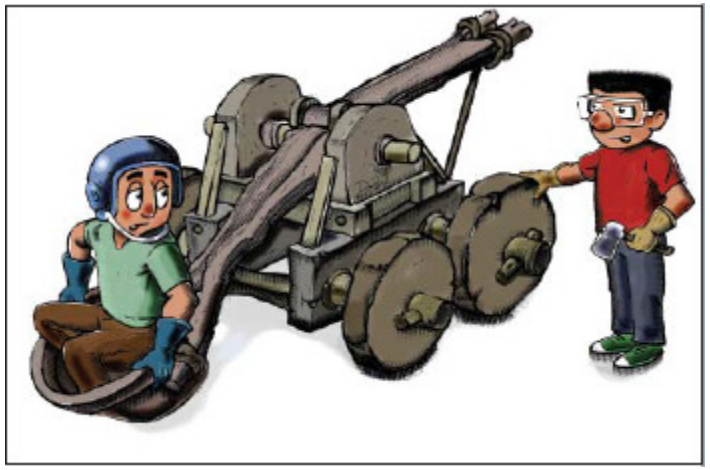
Summary

- **By using a structured approach to incorporate operational risk considerations into the engineering process, evolving mission and business risks are considered and mitigated increasing the likelihood of fielding an operationally effective system, component or capability**



Next Steps

- Use of ORDERED process and/or concepts of operational risk management on critical programs
- Evaluation of results
- Evolution of the ORDERED process based on use and learning



Interested in Advancing Research in Applying Operational Risk Concepts to Systems Engineering?

- **Looking for *individuals*, *programs* or *organizations* interested in applying the ORDERED process and sharing results**
  - Characteristics of Individuals:
    - Interested in exploring operational risk management concepts
  - Characteristics of Programs:
    - Software-intensive or complex service delivery
    - Operational uncertainty during development
  - Characteristics of Organizations:
    - Operational organizations looking for structure operational risk identification process to influence system development
- **Contact:**

  Brian Gallagher

  brian.gallagher@colostate.edu

Questions?

Selected References

- Aronin, B.S., et al., *Expeditionary Combat Support System: Root Cause Analysis*. 2011, DTIC Document.
- Carney, David J., and David Biber. *The Adventures of Ricky & Stick: Fables in Software Acquisition*. Carnegie Mellon University, Software Engineering Institute, 2006
- Carr, M.J., et al., *Taxonomy-based risk identification*. 1993, DTIC Document.
- Ellis, R.F., R.D. Rogers, and B.M. Cochran, *Joint Improvised Explosive Device Defeat Organization (JIEDDO): Tactical Successes Mired in Organizational Chaos; Roadblock in the Counter-IED Fight*. 2007, DTIC Document.
- Gallagher, B.P., et al., *A Taxonomy of Operational Risks.* 2005.
- Gallagher, B.P., *Interpreting Capability Maturity Model Integration (CMMI) for Operational Organizations.* 2002.
- Gallagher, B., et al., *CMMI for Acquisition: Guidelines for Improving the Acquisition of Products and Services*. 2011: Addison-Wesley Professional.
- McCain, J. *FLOOR REMARKS BY SENATOR JOHN MCCAIN ON THE AIR FORCE'S ECSS PROGRAM*. 2014 [cited 2015 2 August, 2015]; Available from: http://www.mccain.senate.gov/public/index.cfm/2014/7/floor-remarks-by-senator-john-mccain-on-the-air-force-s-ecss-program.