Team #1:
Information Technology Software

Team Leads:

Ms. Amanda Graham, Boeing

Mr. Jody Cox ODASD (SCI)

1. Information Technology: scenario description

Scenario:

- As the Director of Communications (J6) for DLA Energy, you are responsible for all communications support for your agency, including hardware and software development, procurement, fielding, and sustainment. Your main IT system Fuels Manager Defense (FMD), a COTS product from Varec, serves as the fuels accountability system of record for DLA. It links to DLA's larger ERP Business System, Enterprise Business System (EBS). FMD is fielded around the world at more than 7,000 sites. It is not only used within DLA, but is also used by the military Services to support many instances of their operations. In total, DLA manages more the $15 billion in fuels sales to DoD, Service, federal agency, foreign military, contractor personnel, and other authorized users regardless of geography or spectrum of conflict. FMD is integral to smooth energy support of key operations.

- Like any large IT system, FMD requires periodic performance and maintenance patches, as well as hardware upgrades. Recently, DLA has identified a need to upgrade FMD's automated fuel tank gauging system with more capable gauging devices. These gauges are COTS products with embedded software that enable it to link to FMD software for easy remote monitoring of product levels and quality. You are going to run a competition for the upgrade with the option for a sustainment contract award.

Apply SCRM process principles (identify, assess, mitigate, and manage) to answer the question: **How can the DoD & Industry better plan for sustainment during Acquisition phase?**

1. What are the sustainment risks/issues associated with your scenario? (List in priority of severity)

2. What proactive sustainment activities would help mitigate risks or resolve issues?

3. For each proactive sustainment activity:
   a) List the information you need during Acquisition phase to plan for sustainment.
   b) List any anticipated systemic constraints or barriers.
   c) Describe how can you can maintain accurate information throughout the system lifecycle?

4. What are the differences in the way we treat repairable versus consumable items?

5. What are the differences in the way we treat systems that are already in Sustainment phases?

1. What are the sustainment risks/issues associated with your scenario? (List in priority of severity)

Risks- (Drivers: Performance, Cost, Schedule)

- Performance, degraded performance
  - Operational failure (inaccurate fuel at the user point of need)
- Cybersecurity (malicious intent)
- Supply Chain
  - Hardware, S/W failure (MTBF disconnect, higher cost, predictability, patch management/upgrades)
  - Obsolescence
  - Counterfeit Parts
- Schedule
  - Preventative maintenance

Issues-

- COTS vs MilSpec mix
- Operational environment/integration
- Operational requirements timing vs funding availability
- Defining the right requirements
  - Gaps, priorities, affordability

2. What proactive sustainment activities would help mitigate risks or resolve issues?

- Monitoring of SC over time (contract for this up front)- visibility
- Planning for the right # of years of operation (can drive obsolescence)
- ID Critical components (risk assessments)
- Design of Supply Chain (resiliency)
- Security requirements flow down
- Collaboration with intelligence community (intel OODA loop)
- Testing plan/requirements
- Planning for technology/capability upgrades
- Transition plan (acquisition to sustainment) engage sustainment conversation up front
- Define data requirements to enable dashboard from production to sustainment

3a. For each proactive sustainment activity:

a) List the information you need during Acquisition phase to plan for sustainment.

b) List any anticipated systemic constraints or barriers.

c) Describe how can you can maintain accurate information throughout the system lifecycle?

- Transition plan to include:
  - BOM, supply chain “map”, QA, performance metrics
  - Criticality analysis of key components
  - Demand/consumption/failure history-performance expectations, lifecycle baseline (to develop requirements)
- Obsolescence/DSMS plan as a deliverable
- Budget/Funding/Manpower targets
- Performance baseline, technology roadmap
- Threat/intel data (risk factors)
- Testing plan to include sustainment considerations

3b. For each proactive sustainment activity:

a) List the information you need during Acquisition phase to plan for sustainment.

b) List any anticipated systemic constraints or barriers.

c) Describe how can you can maintain accurate information throughout the system lifecycle?

- Time
- Money
- People
- Availability of information/supply chain visibility
- Communication/incentives
- Modeling & Simulation tools
- Technology maturation
- Adversarial advancement/persistence

3c. For each proactive sustainment activity:

a) List the information you need during Acquisition phase to plan for sustainment.

b) List any anticipated systemic constraints or barriers.

c) Describe how can you can maintain accurate information throughout the system lifecycle?

- Digital Thread
  - Common database/DLA designated purchased item
- Mandate industry standard requirements (GIDEP, etc)
- Transition plan/systems from acq to sustainment (seamless handoff)
  - Asset visibility, inventory management systems
- Control access/config control/data (collection) integrity, system maintenance
- Continuity of Operations/resiliency plan
- User training

4. What are the differences in the way we treat repairable versus consumable items?

- We don’t have consumables in our scenario
- Unique aspects of software
  - COTS vs development
  - Requirements
  - Upgrades
  - Patch management
  - Configuration management
  - Level of integration
  - Interoperability

5. What are the differences in the way we treat systems that are already in Sustainment phases?

- More “cavalierly”
- Likely to be more vulnerable to new threats because of “older” systems/components
- Less attention/oversight vs acquisition programs
- Programs on “auto-pilot”
- Lower appetite to spend money
- Reactive vs proactive attitude
- Less opportunity to affect (major) change

Team Summary, Insights, Take-aways

- FMD is a key enabling combat support system and expected to work
- Likely that lots of money to reduce cyber risk won't be spent (probably considered a lower risk system)
- Assumption that performance problems in the past will be addressed during the upgrade
- Hardware and commercial software are entry points for bad actors to infiltrate your system
- System architecture- physical, data fusion, transmission, dashboard (how you define this will shape your risk identification and mitigation processes)
- More conversation between the 2 and the 4 (ask for critical components analysis, risk trees, Program Protection Implementation Plan (PPIP))

- How much risk are you willing to pay to mitigate?

- Stay paranoid- assume they're after you because they are!

- Initial thoughts: POV matters, acq vs contractor vs user
- Remediation of compromised parts
- What to add in requirements?
  - Do we need full supply chain visibility and traceability?
- Do we want/can we afford to map the supply chain and require supply chain visibility

Appendix 1:
October 2015 Workshop Findings

- Sound decisions are impeded by lack of supply chain visibility;
- Total supply chain mapping early in process could facilitate better decisions;
- Supply chain ownership changes throughout process and is not clearly defined, nor is the decision authority;
- Technical data package ownership should be addressed in program's initial acquisition plan but may not need to be purchased in the initial phase;
- Flexibility is constrained by available suppliers with proper credentials, but supplier qualification is beneficial even if it results in reducing the supplier pool;
- Malicious actions against the supply chain need to be considered as part of acquisition plan;
- Partnerships reduce risk and cost but must be carefully constructed early in process; and,
- Effective decisions should be made on a cost-benefit outcome, and should be added to our next workshop.