Team #2:
Commercial Electronics

Team Leads:

Ms. Jennifer Bisceglie, Interos Solution Inc

Mr. Andrew Meighan DLA

2. Commercial Electronics:

Department of Defense (DOD) agencies and contractors submitted 526 suspect counterfeit parts reports in the Government-Industry Data Exchange Program (GIDEP) from fiscal years 2011 through 2015, submitted primarily by contractors. Defense agencies and contractor officials explained that congressional attention to counterfeit parts in 2011 and 2012 led to increased reporting, and that the lower number of reports in more recent years is partly the result of better practices to prevent the purchase of counterfeit parts. (United States Government Accountability Office, GAO-16-236)

We are evaluating the purchase of parts for a SCADA system that has been deployed for some time. We have been tasked to consider risks in the supply chain when we evaluate our options and offerors.

Scenario:

The Program Office has let the contracting office know that they have worked with the contractor in the past and purchased multiple products and services from Supplier A for use in SCADA and Substation environments. The Program Office us currently in the process of putting their requirements together for a new procurement and conducting market research to ensure they have followed all necessary DFAR processes. The specific product in question is relay and monitoring equipment for use in electrical industrial control systems and SCADA environments. Those relays rely in some instances on base code / software provided by other third party suppliers. The products are commercially by multiple contractors besides Supplier A. Additionally, Supplier A and their competition supply other entities including many private electricity providers and producers in the electrical industry. Supplier A's customers include the U.S. Department of Defense, U.S. Department of Energy, U.S. Department of Homeland Security, U.S. Army Corps of Engineers, and the Veterans Administration, as well as several municipalities and state governments. During their supply chain risk assessment, if was found that Supplier A purchases code from Supplier B and Supplier C – both located in European (friendly) countries. The supply chain risk assessment also identified vulnerabilities in August 2013 and mitigated by Supplier A. Subsequent reports from 2013 and 2014 indicate that the vulnerability Supplier A mitigated originated with software or code provided by one or more its third-party software suppliers Supplier B and Supplier C.

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)

- Cyber hack
- Change mgmt/version control of the software or hardware
- Traceability and proofing of tiers of suppliers
- Obsolesce of suppliers and supplies
- Lack of influence over suppliers

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

- Request a sustainment plan that vets suppliers based on an agreed to level of criticality of the program
- Update risk mitigation rigor in requirements documents
- Design-in supply chain risk mitigation steps into the product before actual production
- Change acquisition processes so that the expectation that the cost includes risk mitigation
  - The Government needs to understand the cost of increasing the level of risk mitigation to take into consideration during acquisition
- Decrease sole source awards (which will increase sources of supply and provide economies of scale)

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?

Include in requirements:

- A sustainment plan that vets suppliers based on an agreed to level of criticality of the program
- Reliability rates, consumption data, etc. as part of requirements
- Expanded vendor vetting to include financials, company ownership concerns

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?

- OEM out of business
- Limited number of new businesses make the required parts or services
- Having to deal with VARs/distributors vs OEMs, directly
- Cost of lifecycle sustainment with the DoD budget
- Overall budget cycle (1 yr money)/threat of CR/etc.

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?

- Require incentivized performance-based system lifecycle periodic reporting
- Automate data feeds as part of contract requirements

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

- As this is a high priority system, we would treat repairables as consumables, i.e. replace and then repair. Focused on safety and 24x7 up time.

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

- **Current issue:** We tend to underestimate the operating cost of systems already in sustainment phases, due to expertise, time, expectations, etc

- **Future based on this scenario:** Automated reporting outputs will be used to modify and project cost in the out years for readiness

Team Summary & Insights

- Recommendations going forward:
  - Understand the risks and threats to the program – and at which phase of the program each would have impact
  - Include in the requirements determination phase whether we want to buy system performance vs system ownership
  - Conduct threat assessments/vendor vetting that are commensurate with the phase of acquisition/sustainment, type of service or product under consideration, criticality of the program and potential of negative activity
  - Use automated reporting to continually re-assess the multi-year cost of the ongoing program and the cost of continuing to repair or cost to replace

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.