Product Session

Identified Risk:

- Lifecycle considerations
  - Obsolescence
  - Comprehensive sustainment requirements
- Protection of Covered Defense Information
- Supply Chain
  - Insufficient visibility into supply chain
  - Risk management paradigm and planning
- Risk of inter-dependent systems
  - System of systems

Tools:

- People
- Process
- Technology
- Enterprise-wide configuration management

Industry Practices:

- DHS US-CERT Threat alerts
- Maintaining a long term support plan throughout the life of the program
- Up to date budget for lifecycle costs within supply chain
  - Extension of lifecycle and exposure to additional risks
- Use of standards
  - Suitable application of standards and subsequent enforcement
  - Analyze and leverage existing standards and identify gaps

Metrics:

- Identify risks tied to supply chain
- Supply chain profile
  - # of overseas providers
  - # of small businesses
  - Financial health
- Expected vs. actual cost
  - Earned value
  - On time / delivery rates
- Track programs based on performance
  - Red/yellow/green evaluation system

Product Session Recommendations

Recommendation

- Supply chain risk management planning
  - Insufficient evaluation criteria within the contract and weighting (Scoring)

- Supply chain risk management paradigm and
  - Lack of government alerts around risk management threats and risks
    - Failure to identify risk management process

Vendor Certification Session

Identified Risk:

- Foreign interests/ownership
- Changes in suppliers/production for components
- Limited government influence on industry actions

Tools:

- Risk management/commercial standards
- Vendor certification and management software

Industry Practices:

- Focus risk management based on business impact
- Leverage standards to reduce reporting/management burden

Metrics

- No consistently applied metrics identified
- In general:
  - Metrics are tiered to risk needs
  - Supplier performance (including risk) is tracked by industry
- General risk metrics include
  - Value at risk
  - Time to recovery

Vendor Session Recommendations

- **Use a tiered approach to SCRM based on item/program criticality and use (one size does not fit all)**
  - SCRM requirements tailored to the level of security needed at each tier
  - Build flexibility on SCRM approach based on security needs
- **Create an understanding of cost vs. risk to allow decisions on paying more for a more secure/visible supply chain**
  - Better understanding of “return” on risk investment
  - Be realistic in what government can reasonably expect from suppliers
- **Greater/consistent gate review analysis of supply chain threat assessments**
  - Ensure compliance with laws and policy
  - Highlight potential risks
- **Improve consistent enforcement and codification of current regulation and policy**
  - Support translation of policy to implementation
  - Ensure policy is enforced and consistently applied

Distribution Session

Identified Risk:

- Defining what is critical is not easy
  - Based on system readiness or distribution/supply chain?
  - When does it matter? Part vs assembly
  - Cost?
- Governance needed to decide who decides what is critical.
- Distribution line risk assessment – link real word events to DoD distribution system

Tools:

- Supply Chain Mapping is key to understanding risk
- Data exhaust – what do we do with it and why?
- Data aggregation – double edge
- Contract clauses - partnership
- Electronic parts traceability (DFARS)

Industry Practices:

- To Mark or Not To Mark?
- Academic Engagement to stay ahead of the curve
- Vendor Direct Shipping has increased risk
- DoD has typically bought down risk via inventory
- Don't forget retrograde
- Government to replicate performance standards when government is LSI

Metrics

- Tracking parts – what does that tell us about system (Detectability)
- Risk Score – balanced role of government and industry

Cyber/IT Session

Identified Risk:

- A – No singular process in place to leverage technology
- B – Multiple, current processes are disjointed, which negatively impacts capture and communication of information
- C – We need to develop a uniform methodology to prioritize risk
- D – Poor transition from acquisition to operations and sustainment

Tools/Capabilities:

- A – Prioritization of missions and programs leading to manufacturers, vendors, and components
- B – Alignment across the processes of what a complete record looks like
- C – Alignment in the process of where the information is captured and whether or not it is captured by a human or automatically
- D – Need feedback and alerting capabilities

Industry Practices:

- A – Industry will be responsive based on requirements and funding
- B – There will be a need to align industry best practices with Navy/DoD requirements

Metrics

- A – Metrics must be outcome-based and must still be defined
- B – Provides information that can inform multi-level decision making
- C – Metrics need to be granular, transparent, and automated

Cyber/IT Session Recommendations

- **Recommendation 1**
  - **Highlight:** Establish who is responsible, what the priorities are, and gain senior leadership buy-in
  - **Issue**: Still working through defining the problem and working through who is going to be responsible
  - **Issue:** What is the business problem we are trying to solve?

- **Recommendation 2**
  - **Highlight:** Leverage CYBERSAFE framework across the Navy and wider DoD
  - **Issue:** Understanding and prioritization of what is mission critical
  - **Issue:** Document existing process gaps and seams