Program Protection Planning: Industry Perspective

What is industry seeing from customers:

- Tell us what you are doing (not how you are going to do)
- Program Managers don't seem to understand what PPP, passing on requirement
- Programs respond to contract, not desired holistic approach
- Lack of understanding in statement of work (e.g. implement full PPP, paragraph on IA, paragraph on AT – what is really being asked?)

Challenge in defining what is needed in a contract

- Follow AT approach for defining requirements (e.g. AT handbook with language)
- Low price vs. protection , need 60% technical, 40% cost
- Consistency issue: everyone interprets PPP contract language differently

Discussion:

- What makes a good systems engineer: System thinking, "kid" that thinks out of the box
- PPP should not be talking about AT, IA, supply chain, etc. – need to focus across all areas
- How do we measure assurance?
- System security engineering in contract refers to a MIL handbook (IA focus)
- Need to have the right system security engineering philosophy
- Need graduated scale – simple things are not expensive (coding principles, don't buy parts from China, etc.) and should be placed on contract
- Professional certifications don't cover the holistic discipline needed
- Breadth is concern – we can harden our systems, but vulnerabilities exist in development environment (supplier that collect data)
- Need to think about all things that interact with our systems (development, manufacturing, test equipment, field updates)
- "Burglar" can learn a lot about system under attack through open
- Prioritize what is critical – what is critical? (every engineer has a different opinion on that)
- Analogy to soccer
    - Midfield line is protecting networks
    - Active defense is the goalie – can do more things and not get "carded"
- What is industry doing to protect their own data?
    - Can't share data (PII) with other companies
    - Should follow gaming industry model of sharing threats
    - Stock price goes down if company is attacked
    - Don't need source and method – just the signature
- Trusted Foundry for trusted supply chain
- How do we know what is being manufactured?
- Internal education need to span all employees (not just engineers)
- Measuring assurance
    - NATO efforts to define metrics for risk based assessment
    - Measure risk reduction
    - Need structured vocabulary and taxonomy (avoid collision of terms)
- Measure value of security investment (not spent right if attacked, too much spent if not attacked)

- Difference between broadcasting and sharing information
- Programs reluctant to have their systems tested – don’t have funding to fix what is found
- Assessment of vulnerabilities does not get to the warfighter
- Electronic Warfare model can work: notify warfighter and allow vulnerabilities to be prioritized and fixed
- Will be exposing vulnerabilities in legacy programs in Systems of Systems testing
- Where is ops tempo to solve SSE problems?
    - Joint DHS/NIST/DoD quarterly meetings that industry can attend (SW/Supply Chain)
    - NDIA SSE Committee meets 4-6 times a year, low industry participation
    - Annual SE conference
    - Need to identify what needs to be done and work it like a program
    - Should engage NDIA SSE Committee with Joint DHS/NIST/DoD
    - Many meetings to “admire the problem”
- Are there changes needed in the PPP?
    - More information about threats
    - Dimensions of supply chain
    - Help government ask for what they need from industry response
    - Vulnerability and threat assessment poorly flushed out
    - Electronic Warfare not addressed in PPP
    - Don’t have conventional threats, directed energy threats, hazards
- Need integrated threat catalog, break down walls between disciplines
- Industry working enablers to address intent of current PPP
    - SSE is a new discipline
    - PPP is done by SSE in collaboration with other disciplines
    - Cyber Security Systems Engineering – how is it architected?
    - SSE need to work with SE in risk based
- Good to see discipline being put into systems security engineering and rigor
- Need to increase ops tempo