Agenda

- DSS in Transition
- Evolving with the Threat
- Time to Evolve the Security Program
- Tailored Security Program Framework
- Identifying Critical Technologies
  - Technology Lifecycle Maps

- Critical Asset Identification
- Tailored Security Plan
- DSS SVA Risk Based Pilot
  - Lessons Learned
- Going Forward
- Conclusion
Thank you

Raytheon Senior Leadership and DSS Western Region team for affording Raytheon the opportunity to collaborate in this new initiative.
DSS in Transition (DiT)

- DSS announced “DSS in Transition (DiT)” November 2016
- Raytheon Company (RMS) is aligned with this new vision and requested to partner with DSS in developing this approach
- Partnership began January 2017 with intent to pilot “Risk Based” assessment approach during September 2017 Security Vulnerability Assessment
- RMS felt strongly this new approach will put the right focus where it matters most

If you protect everything… you protect nothing!
Evolving with the Threat

• The United States is now facing the most significant foreign intelligence threat it has ever encountered.

• Adversaries are successfully attacking cleared industry at an unprecedented rate.

• They are using multiple avenues of attack, varying their methods, and adjusting their priorities based on the targeted information they need.

• As a result, they are upgrading their military capabilities and competing against our economy using the very same information they stole from cleared industry.
Time to Evolve the Security Program

Layered Security Program

- Document
- GSA Safe
- Closed Area
- Secured Building
- Security-in-Depth

Where is the risk?

Check the Box Security
Tailored Security Program Framework

- Six Sigma Project Started in January 2017
- Necessary Stakeholders
  - Leadership
  - Functional Organizations
  - Supplier Base
  - Employees
  - Defense Security Service
  - Customer
- Asset Identification
  - Critical Technologies
  - Subject Matter Experts
  - Programs
  - Suppliers
  - Infrastructure
  - Processes
Identifying Critical Technologies

- Department of Commerce Survey
- Senior Leadership – Engineering
  - Engineering knows what is a critical asset to national security
- Created Critical Technologies List
- Built Technology Lifecycle Maps
- Identified suppliers associated with critical technologies
- Critical Program Information Identified by Customer

<table>
<thead>
<tr>
<th>CRITICAL TECHNOLOGIES LIST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical Technology</td>
</tr>
<tr>
<td>------------------------</td>
</tr>
</tbody>
</table>

Technology Lifecycle Maps – Full Lifecycle of Protection
Technology Lifecycle Maps

- Technology Maps created to determine full lifecycle to ensure protection from beginning to end.

**Subcomponent – Received Externally**
- Part 1 Name, Supplier, Cage
- Part 2 Name, Supplier, Cage
- Part 3 Name, Supplier, Cage
- Part 4 Name, Supplier, Cage

**Internal Processing – Closed Area/Space 1**
- Component 1
  - Next stage of build up

**Internal Processing – Closed Area/Space 2**
- Component 2
  - Next stage of build up

**External Transmission**
- Where does it go when Leaves?
  - Next stage of build up/delivery

Part 1-4 – Key words – define what is critical to protect
Component 1 – Key words – define what is critical to protect
**Critical Assets Identification**

### Programs
- Programs that are critical to national defense
- Horizontal protection
  - Critical component on one program used on others – must be protected in all areas used

### Infrastructure
- Cost/Time to replace
- Inability to replace impacts national security
- Time to replace creates a vulnerability to national security
  - Building loss/compromise would stop production leaving a vulnerability to a defense system/customer.
Critical Assets Identification (cont.)

<table>
<thead>
<tr>
<th>Suppliers</th>
<th>Personnel</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Critical Suppliers identified by critical components and programs</td>
<td>▪ Critical skill sets</td>
<td>▪ The “how to” or “secret sauce” to why something is critical</td>
</tr>
<tr>
<td>• Sole source – Only source for product</td>
<td>▪ Succession planning/replicability</td>
<td>▪ Something unique through a process that impacts effectiveness</td>
</tr>
<tr>
<td>• Single source – Only source approved by customers</td>
<td>▪ What happens when they leave?</td>
<td></td>
</tr>
<tr>
<td>• New source 3 months - 5+ years &amp; significant financial investment</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Tailored Security Plan

- Concept of Operations
- Family of Controls
- Risk Register
- Technology Mapping
- Metrics / Dashboard
- Risk Based Employee Questionnaire
- DSS Provided Threat Data

Scalable & Repeatable
The DSS Security Vulnerability Assessment (SVA) introduced a risk-based overlay to the traditional assessment focusing on critical assets.

Week prior to the SVA they reviewed traditional elements:
- i.e. Training/Education, Self-Inspection results/mitigation strategies, document control.

DSS focused on critical assets and followed technology lifecycle maps.

DSS looked at all findings/observations and asked “What is the risk?”

Training is needed on both sides to implement this new model.

Critical to evaluate current and new programs for changing critical technology.

Currently no oversight for uncleared suppliers providing critical components.
Going forward

- Ongoing collaboration with DSS and customers
- Recurring DSS in Transition Working Group meetings
- Enhance risk register and technology mapping capabilities
- Develop predictive analysis dashboard
- Establish supplier oversight
  - Security Manager assigned to Supply Chain
  - Develop supplier assessment model
  - Provide oversight to uncleared suppliers
- Change Management
  - Leadership engagement
  - Employee culture
  - Risk based vs. “check the box”
Conclusion

- Leadership “buy in” key
- Resources targeted at what is critical vs. everything
- Cost effective security process/programs
- Builds customer confidence
  - Ensures we are delivering products that are not compromised
  - Protecting the warfighter
- Protects the company and brand
Contact Information

- **Greg Garcia**  
  Sr. Manager, Industrial Security  
  (520) 794-2929 desk  
  (520) 440-6281 cell  
  gagarcia@Raytheon.com

- **Heather McDowell**  
  Facility Security Officer  
  (520) 794-0305 desk  
  (520) 471-6813 cell  
  heather.mcdowell@Raytheon.com

- **Andy Lewis**  
  RMS Operations Manager  
  (520) 794-0666 desk  
  (520) 307-7658 cell  
  Andy.lewis@Raytheon.com