LOCKHEED MARTIN

Presentation for Aerospace & Defense Coalition

Supply Chain Cybersecurity

LOCKHEED MARTIN

People

- 97,000 Employees
- *60*,000 Scientists, Engineers and IT Professionals
- 500+ Facilities *Across the US*
- *And Operating in 70* Countries

Customers

- Departments of
  - Defense
  - Homeland Security
  - Commerce
  - Energy
  - Health & Human Services
  - Housing & Urban Development
  - Justice
  - State
  - Transportation
- NASA
- Social Security Administration
- Environmental Protection Agency
- U.S. Postal Service
- Intelligence Communities
- 70 other Governments Worldwide

We Never Forget Who We're Working For ®

Lockheed Martin Corporation

ROTARY AND MISSION SYSTEMS
- Radar and surveillance systems
- Training and logistics solutions
- Simulation technologies

AERONAUTICS
- Tactical fighters
- Tactical and strategic airlift
- Advanced Development

SPACE SYSTEMS
- Surveillance and navigation
- Global communications
- Human space flight
- Strategic and defensive systems

MISSILES & FIRE CONTROL
- Air and missile defense
- Fire control and situational awareness
- Nuclear systems and solutions

CORPORATE HEADQUARTERS
- Bethesda, Maryland

Qualities We Look for in a New Supplier...

- Socio-economic status
- Past performance with federal customer
- Experience with Lockheed Martin or Prime Contractor
- Quality certifications
- Location
- Technology and Innovation
- Supplier of needed services
- ***Cybersecurity Ready***

Supply Chain Cyber Initiative Strategy

Understand Posture
(Questionnaires & Validations)

Build Awareness

Reduce Risk

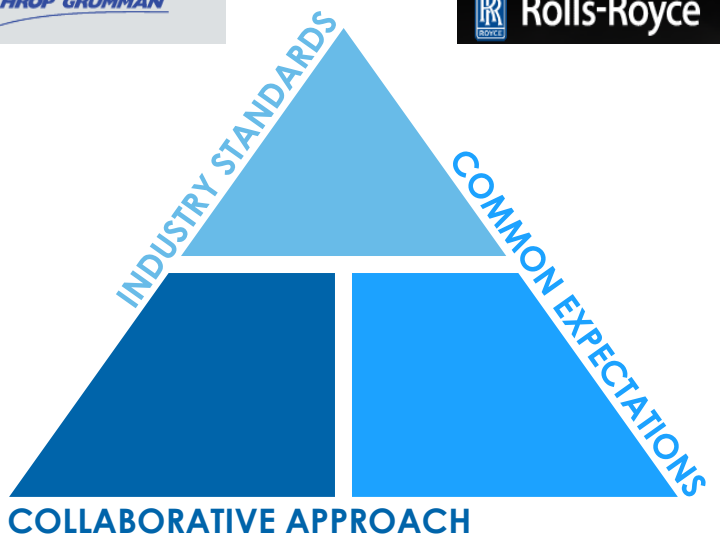
Collaboration

- ❑ Supply Chain
- ❑ Cyber Security
- ❑ Program Management
- ❑ Engineering

End Goal

- ❑ Compliance w/ Cyber DFARS
- ❑ Broad cyber risk assessment, awareness and education
- ❑ Risk-based cyber mitigation actions
- ❑ Supplier Threat awareness and Monitoring… Self-Reporting to LM/DoD

Industry Collaboration & Supplier Engagement



- LM chairs the Supply Chain Cybersecurity Working Group
- Exostar hosts cybersecurity questionnaires
- Common supplier expectations
- Supplier inputs once, results shared across multiple primes

Understand Supplier Posture

Cybersecurity Questionnaire

- 180 questions
- APT and risk focus
- Developed by Exostar partners
- Based on standards: Center for Internet Security top Critical Security Controls

NIST 800-171 Questionnaire

- 110 questions
- Compliance for Covered Defense Info (CDI) as defined in DFARS 252.204 - 7012
- Regulatory compliance by 12/31/2017

Lockheed Martin's Expectations of our Suppliers

- **Assess internal cybersecurity maturity using Exostar questionnaire(s)**
  - **Handling Sensitive Information**
    - Complete the Cybersecurity Questionnaire (180 questions)
    - Result: ~40 page report with Rating/Scores and links to recommendations
    - Define a remediation plan and work to close on open items
  - **Handling Covered Defense Information (CDI) as defined by DFARS**
    - Be aware of applicable DFARS clauses in LM CorpDocs
    - Flow DFARS requirements to sub-tier suppliers
    - Complete the NIST 800-171 Questionnaire (110 questions)
    - Be compliant by December 31, 2017
    - 30 Day notification to DoD CIO and LMC of non compliant NIST controls
    - Report cyber incidents within 72 hours to DoD CIO and LMC

Supplier Takeaway

- As an LM supplier you are a target of our adversaries
- Lockheed Martin is working with suppliers:
  - To understand their cybersecurity posture
  - To bring a heightened sense of cybersecurity awareness
- Suppliers are responsible
  - To complete the Cyber Security Questionnaire
  - To complete the DFARS/NIST 800-171 Questionnaire if applicable
  - To improve their cybersecurity posture as necessary
  - To be compliant with NIST 800-171 by December 31, 2017 (if applicable)

Supply Chain Resources

- **Supplier Accessible Support Sites**
  - Lockheed Martin External website for Supply Chain Cyber
    - http://www.lockheedmartin.com/us/suppliers/cybersecurity.html
  - Exostar PIM Cybersecurity Questionnaire and Supplier Process FAQs
    - http://www.myexostar.com/Questionnaire-Resources/
    - Exostar Resource Center for NIST 800-171