BAE Systems, Inc.

DFARS Cybersecurity Compliance Program Management Approach

NEW HAMPSHIRE MANUFACTURING EXCHANGE PARTNERSHIP
June 29, 2017

Cathryn Jackson, Director, Supply Chain Cybersecurity Program
Paul Kling, Director III, Operations, Electronic Systems

BAE SYSTEMS
INSPIRED WORK

BAE Systems, Inc.
Cybersecurity DFARS Compliance Program

AGENDA*

- Company Overview and Values
- What is the DFARS?
- How is BAE Systems, Inc. Doing It?
- DFARS Compliance Management Approach
- Supply Chain Flow-down
- Q & A

This presentation is not intended to provide legal advice; please consult your legal counsel on compliance requirements

BAE Systems:
A commanding breadth of capabilities

ELECTRONICS

MARITIME

LAND

INTELLIGENCE

SUPPORT SERVICES

- BAE Systems is a global defense, aerospace and security company
- Over 83,000 employees worldwide
- Delivers a full range of products and services for air, land and naval forces, advanced electronics, security, information technology solutions and customer support and services
- Over 2,100 U.S. and foreign patents across numerous technology domains
- **Over 25,000 Supply Chain business partners/suppliers**

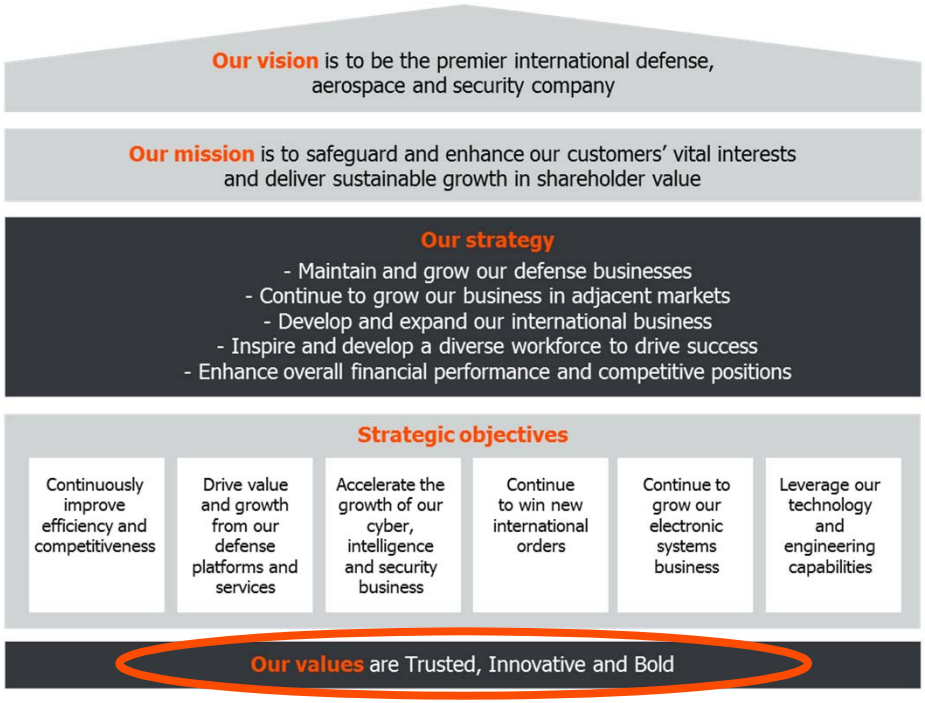
BAE SYSTEMS
INSPIRED WORK

BAE Systems is committed to its values

Trusted – we deliver on our commitments
- We are honest and take responsibility
- We can be relied upon
- Everyone matters

Innovative – we create leading-edge solutions
- We value imagination and experience
- We empower teams
- Working together we turn our ideas and technologies into solutions

Bold – we constructively challenge and take the initiative
- We operate with tenacity and resolve
- We accept challenges and manage risk
- We set stretching goals



BAE SYSTEMS
INSPIRED WORK

Why Elevated Cybersecurity Compliance Requirements?

- **Increase in frequency and sophistication of cyber attacks can cause**
  - Business disruption
  - Loss of Confidentiality, Integrity or Availability of DoD data
- **Loss of unclassified defense technology and/or information could impact**
  - National Security
  - US competitive technological advantage
  - US and allied warfighters
- **DoD contractors and suppliers need to enhance the protection of their unclassified systems and data**

"July 6, 2016, House Committee on Small Business Chairman, Steve Cabot, brought up the risk of cyber-threats on small businesses. Although foreign actors are a major threat, 71% of cyber-attacks happened to businesses with less than 100 employees."

DFARS Compliance

WHAT IS THE DFARS?

The Defense Federal Acquisition Regulation Supplement (DFARS) to the Federal Acquisition Regulation (FAR) is administered by the Department of Defense (DoD). The DFARS contains requirements of law, DoD-wide policies, delegations of FAR authorities, deviations from FAR requirements, and policies/procedures that have a significant effect on defense contractors.

WHAT IS DFARS CYBERSECURITY COMPLIANCE?

Developing processes, procedures and tools to insure suppliers' compliance with DFARS requirements for the protection of Controlled Defense Information (CDI), Controlled Technical Information (CTI), and Controlled Unclassified Information (CUI).

DFARS Compliance – What is CDI?

National Institute of Standards and Technology (NIST) 800-171 standards are a set of requirements that safeguard **Covered Defense Information** and mandate Cyber Incident Reporting for companies that have entered or will enter into DoD contracts or subcontracts.

Covered Defense Information (CDI)

- Unclassified controlled technical information (CTI) or other information (as described in the CUI Registry) that requires safeguarding or dissemination controls … **AND is [either]**
  - (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to contractor by or on behalf of, DoD in support of the performance of the contract; **OR**
  - (2) Collected, developed, received, transmitted, used, or stored by, or on behalf of, the contractor in support of the performance of the contract.

DFARS COMPLIANCE REQUIREMENTS
Government Directives History*

Anticipate additional FAR release

2013 | 2014 | 2015 | 2016 | 2017 | 2018

Nov 18, 2013

Aug 26, 2015

June 16, 2016

Oct 21, 2016

Dec 31, 2017

DFARS Final Ruling
- *Does not apply to COTS*
- *Tied CDI to CUI Registry*
- *Subs to notify next higher tier when requesting Deviations from NIST SP 800-171*
- ***NIST SP 800-171r1*** *released Dec 20, 2016 increased to 110 controls (added System Security Plan requirement)*

DFARS compliance deadline

FAR 52.204-21 *BASIC SAFEGUARDING OF CONTRACTOR INFORMATION SYSTEMS REQUIREMENTS*
Does not apply to COTS
15 requirements (corresponding to 17 of the 109 NIST SP 800-171 requirements)
Expanded to include Federal Contract Information

Basic Safeguards Extended to ALL Federal contracts
(affecting over 300K companies)

DFARS 252.204-7012
Expanded to Covered Defense Information (CDI)

Expanded to ALL Defense contracts
(affecting over 13K companies)

DFARS 252.204-7012, *Safeguarding Unclassified Controlled Technical Information (UCTI)*

Selected controls from the NIST 80-53r4

Required in Defense contracts with UCTI to:

· Protect Unclassified (UCTI) Data · Report Cyber Incidents · Flow-down to Subcontractors

** Excerpts From the AIA DFARS Overview*

BAE SYSTEMS
INSPIRED WORK

BAE Systems' DFARS Compliance Program

Compliance Management Approach for Internal Systems

- Identification of all systems holding CDI data
  - Identify specific leads / POC's for each program or environment
  - Separate production and non-production computing environments
- NIST Control Assessments
  - Complete a NIST 800-171 compliance survey against the described assets
  - Perform Program Gap Analysis - score against the 110 controls for each of the programs and which controls are non-compliant
- Plan of Actions and Milestones
  - Create POA&Ms to identify areas of non-compliance, define mitigation strategies to reduce the risk, and resolve areas of non-compliance
- Track Population
  - Track compliance status by system, program, and computing environments

BAE Systems' DFARS Compliance Program

Compliance Management Approach for Supply Chain

- Steering Committee and Program Director assigned to provide corporate prioritization, continuity and oversight
- Identified Sector Program Managers for each business sector
- Team developed a 5 Phase Roadmap and PMs manage execution
  - Phase 1 – Planning
  - Phase 2 – Risk Assessment
    - Prioritize supply chain based upon 10 risk criteria
    - Request Suppliers' DFARS compliance status via 4 question Supplier Affirmation Letter
  - Phase 3 – Supplier Compliance Evaluation
    - Communicate to determine supplier's compliance intent: Yes, No, Never
  - Phase 4 – Mitigation Options
    - Review results with suppliers unable to meet deadline
  - Phase 5 – Compliance Sustainment Plan
- Track and report progress with a Master Scheduler

BAE Systems, Inc.
DFARS Requirements Flow-down to Suppliers

Department of Defense requires that DFARS compliance requirements are flowed-down to supplier/subcontractors

- All Primes must flow down to all Subcontractors who will handle CDI data
- Subcontractors are required to flow-down the requirement to their suppliers if they will handle CDI
- All BAE Systems Terms and Condition statements have been modified to included the new DFARS requirement, when applicable
- DFARS compliance is the responsibility of the individual supplier, not the prime

DFARS COMPLIANCE CHALLENGES

- **Compliance Assessments can be complex**
  - 110 NIST controls must be applied to all systems handling CUI
  - Process could become expensive to meet all standards by Dec 31st
- **Schedule Constraints**
  - Large Supply Chain to cover in a fixed amount of time
  - Supplier response to Affirmation Letter critical to program staying on schedule
- **Resource Constraints**
  - Technical expertise needed
  - Number of non-compliant suppliers could exceed resources available to mitigate
- **100% DFARS compliance may not be achievable by all suppliers by deadline (currently 31 December, 2017), or even possible for some suppliers**

Questions?

Backup Slides

BAE SYSTEMS
INSPIRED WORK

DFARS Compliance – What is the NIST 800-171?

- 110 technical, procedural, management, and physical requirements for information systems housing CUI
- Categorized into 14 groups

- Access Control
- Awareness And Training
- Audit And Accountability
- Configuration Management
- Identification And Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System And Communications Protection
- System And Information Integrity

Identified Most Challenging Requirements

- The Aerospace Industries Association (AIA) surveyed suppliers to identify the most difficult and costly requirements to implement.

Rating	Difficulty	Cost
1	• Multifactor authentication	• Multifactor authentication
2	• FIPS encryption of CUI	• FIPS encryption of CUI
3	• Software whitelist/blacklist	• Software whitelist/blacklist
4	• Review audit logs	• Control CUI flow within system • Mobile device encryption • System audit record retention • Multifactor remote sessions
5	• System audit record retention • System clock synchronization • Maintain system and software baseline configurations • Periodically assess Risk	• Review audit logs • Encrypt CUI on digital media