DoD Office of Small Business Programs

USD (A&S)

DoD Mid-Atlantic Regional Council Summer 2020 Workshop
Small Business Office Accomplishments

*Small Business Outreach Events: 5,300*

*Small Businesses Trained: 54,000*

*Small Business Training Week: May 2019*

*DoD Small Business Awards:*$160 Billion (Prime/Sub) FY 2019*

*Small Business Cybersecurity Trainings: 7,000+*

*Small Business Jobs Created: 654,000*

*Small Business Strategy*

*SBA Procurement Scorecard (FY 2014-2018)*

*Small Business Office Accomplishments*
DoD Small Business Performance
FY 2019

Small Business Eligible Dollars
$312,233,095,170

Small Business Dollars
$75,422,792,714

Small Business Achievement / Goal
24.16% / 21.80%

Data Source: FPDS-NG as of 2/20/2020 Using FY2019 Small Business Goaling Exclusions, Overall Data using Funding Department ID 9700 / Component Data using Contract Awarding Department 9700
DoD Component $ by Category
FY 2019

Total $

- ARMY: $75.8B, $22.1B, 29.18%
- NAVY: $89.8B, $16.8B, 18.66%
- AIR FORCE: $65.5B, $13.0B, 19.77%
- DLA: $38.5B, $15.0B, 38.87%
- ODAs: $28.5B, $6.8B, 23.87%

Data Source: FPDS-NG as of 2/20/2020 Using FY2019 Small Business Goaling Exclusions, Overall Data using Funding Department ID 9700 / Component Data using Contract Awarding Department 9700
• Under the authority of NDAA 2019 Sec. 1644: Assistance for small manufacturers in the defense industrial supply chain and universities. 
  (a) DISSEMINATION OF CYBERSECURITY RESOURCES.
  (b) VOLUNTARY CYBERSECURITY SELF-ASSESSMENTS.
  (c) TRANSFER OF RESEARCH FINDINGS AND EXPERTISE.
  (d) DEFENSE ACQUISITION WORKFORCE CYBER TRAINING PROGRAM.
  (e) ESTABLISHMENT OF CYBERSECURITY FOR DIB MANUFACTURING.

(f) AUTHORITY.--In carrying out this section, the Secretary may use the following authorities: (1) The Manufacturing Technology Program established under section 2521 of title 10, United States Code. (2) .... (3) ...(4) The Small Business Innovation Research program. (5) The mentor-protege program. (6) Other legal authorities as the Secretary determines necessary to effectively and efficiently carry out this section.

• Compliance with existing regulations, DFARS clauses (252.204-7008, 252.204-7012) which requires compliance with NIST SP 800-171, safeguarding of defense-relevant information, and cyber incident reporting.
• Awareness of evolving rules and standards such as the proposed CMMC.
Project Spectrum

- Project Spectrum events and programs will enhance awareness of cybersecurity threats within the manufacturing, research and development, as well as knowledge-based services sectors of the industrial base.
- Project Spectrum will leverage strategic partnerships within and outside of the DoD to accelerate the overall cybersecurity compliance of the DIB.
- [www.Projectspectrum.io](http://www.Projectspectrum.io) is a web portal that will provide resources such as individualized dashboards, a marketplace, and Pilot Program to help accelerate cybersecurity compliance.
“What’s the difference between NIST 800-171 & CMMC?”

- NIST 800-171 compliance practices are all factored into CMMC with industry wide additions at higher levels.
- NIST 800-171 is **not** going away! It is merely being factored into CMMC with industry wide additions at higher levels.
Project Spectrum Big Picture

**Baseline:**
Readiness check indicates current self attested compliance on NIST and CMMC, output is a graphic with a level check.

- Outreach to other DoD Programs that support small business
- Outreach to small business via PTACS
- Outreach to small business via Industry Assoc.

**Dashboard by Company**
- Marketplace, eTools, other means to stay compliant

**Training Resources**

**PS Pilot Program**
Coaching and access to tools we offer at reduced cost.

**Results in measurable increased compliance**

**PS Web Portal audience is small business**
Project Spectrum Partnerships

- Collaborate across industry associations, the Manufacturing Innovation Institutes, and the Mentor-Protégé Program

- Engage partners and infrastructure that already exists and to rapidly stand-up a national capability focused on cybersecurity
Mentor Protégé Program
Industry Partnerships

- Boeing
- Raytheon
- Rockwell Collins
- BAE Systems
- CACI
- Parsons
- Booz Allen Hamilton
- General Dynamics
- L3Harris
- Jacobs
Cybersecurity Pilot Program Objectives

- Enroll MPP and other select companies
  - Manufacturing, Research and Development, and Knowledge-based services sectors
  - Possess the necessary resources to respond to vulnerabilities identified during the pilot
- Increase MPP participants compliance and cyber incident reporting
- Foster measurable increases in security awareness
- Provide exclusive training, tools, and advisory services to existing and new MPP participants
- Initial cohort of at least 25 companies targeted for enrollment approx. every 120 days
  - Must agree to 24 month collaboration and information exchange with DoD
• Manufacturers often use legacy equipment which presents challenges that are harder to patch vulnerabilities and protect from attack.

Unique issues manufacturers face
• Also manufacturers use OT and IOT plant equipment which requires sensors being placed on the network to gather vulnerability data.
• Often multiple geographic locations.
• Do not have on site IT support staff.

Benefits to manufacturers
• Cost conscious tools to assess gap vulnerabilities and link to patches
• Vetted Marketplace to find solutions
• Company dashboard to track compliance journey
• Most recent information on cyber issues
• Reduce cost of compliance NIST/MEP

Pilot Program
Training Modules
Tool Prototyping
Sensors on the network to assess vulnerabilities/Compliance Management Coach
Who they are:
Innovator/Scientist/Researcher/ Startup
• Individual contributors/entrepreneurs
• No company infrastructure
• Limited funding
• Funding largely focused on technology
• Often wholly unaware of DoD acquisition requirements
• Often non-traditional business

Labs & Corporate Spinouts/ Venture-backed & Mature small businesses
• Often commercial business-oriented
• Cybersecurity posture driven primarily by minimal requirements
• May have limited resources allocated to IP and data protection
• Rich targets for acquisition

Designed to address unique R&D performer challenges
### Unique to Advisory and Assistance Services (A&AS):

- Support R&D and Manufacturing sectors
- Number of employees can be as few as one
- Remote environments
- Cloud data
- Varied software platforms
- Need to collaborate into an existing business workflow

### Marketplace of platforms for secure collaboration

### Create cybersecurity awareness

### Community of many for those who are few
Cybersecurity Pilot Program Outcome

- Pilot companies show measurable increase in security awareness.
- Pilot companies show increase in NIST SP 800-171 compliance.
- Pilot companies demonstrate readiness for CMMC accreditation.
- Best practices shared among DoD small business community.
- Continuous engagement with DoD small businesses for valued services.
Cyber Security Project Spectrum Initiative Outcome

**EDUCATE**
- 10,000
  - Individuals trained with Live and Web-Based Training

**INSTILL BEST PRACTICES**
- 100
  - MPP participants engaged with individualized solutions

**CREATE COMMUNITY**
- 100,000
  - Active users of web portal

**DEVELOP SOLUTIONS**
- 500
  - DIB firms using prototype tools
Summary

- OSBP is working closely with the CMMC Accrediting Body to prioritize NDAA Sec. 1644(f) program participants.

- OSBP is providing preparedness training for future CMMC compliance and a pilot program that seeks to prepare those companies for CMMC certification.

- Project Spectrum will include a vetted, competitive marketplace to assist small businesses with finding local solutions.

- OSBP is approaching this effort understanding cybersecurity is a business calculus for many companies in the defense supply chain.

- OSBP will help companies understand how strong cybersecurity helps protect data and mitigate business risks associated with unsecured networks.