MARYLAND DEFENSE CYBERSECURITY ASSISTANCE PROGRAM

MARYLAND MEP
MANUFACTURING • EXTENSION • PARTNERSHIP

Montgomery County Chamber of Commerce
February 22, 2019

About MD MEP

MARYLAND MEP
MANUFACTURING • EXTENSION • PARTNERSHIP

Maryland
DEPARTMENT OF COMMERCE

About the Maryland MEP

- Independent Non-Profit Organization
- Mission
  - To advance manufacturing in Maryland by making ALL manufacturers in the State; **stronger**, **smarter** and **more profitable**.
- Work with manufacturers throughout the State of Maryland

Part of a National Network of Centers

National Program to grow manufacturing in the US through Public and Private Partnership

Affiliate of National Institute of Standards and Technology (NIST) Manufacturing Extension Partnership (MEP) National Network

*Only federal program with client reported impacts

Cybersecurity – An MEP National Network Initiative

- Pilot Programs created to support manufacturers with compliance
- Standardization of resources and tools for assistance
- Dissemination of knowledge and methods

- MD MEP Cyber Program
  - 2017 Pilot to Work with Air Force SBIR Companies
  - 2017 Pilot to Work with Small and Mid-Sized Manufacturers
  - Development of scalable assessment program for defense contractors
  - Identification and use of local partners and resources
  - 2018 Development and Launch of the Maryland Defense Cybersecurity Assistance Program (DCAP)

Why Cybersecurity?

MARYLAND MEP
MANUFACTURING • EXTENSION • PARTNERSHIP

Maryland
DEPARTMENT OF COMMERCE

U.S. Manufacturers Are Prime Targets for Cyberattacks, Report Says

By Paul Huang

September 25, 2017 5:12 pm Last Updated: September 25, 2017 5:18 pm

News › Business › Business News

Equifax reveals 15.2 million client records were compromised in massive cyber attack last month

Breached records included sensitive information affecting nearly 700,000 consumers

John McCrank | Wednesday 11 October 2017 09:02 BST | 0 comments

2 shares

Like Click to follow The Independent Online

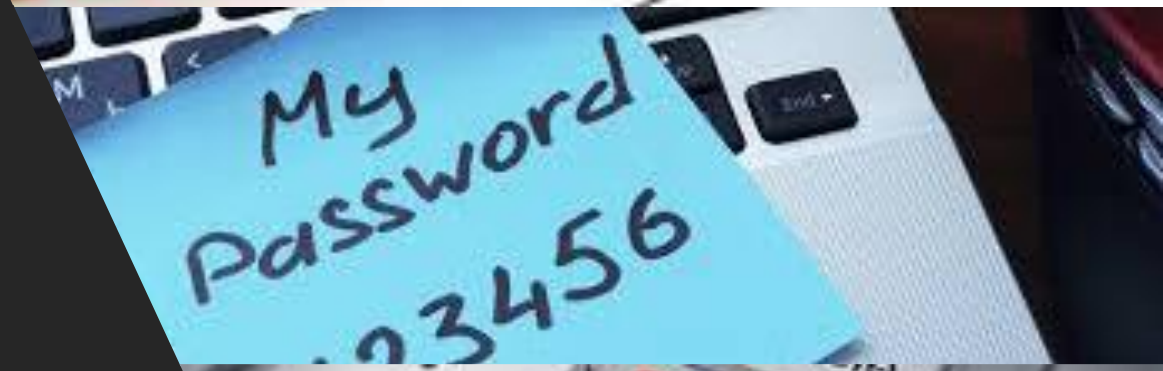
UK manufacturers fall victim to cyber attacks, survey reveals

80 UK manufacturers subjected to cyber attacks but many more may have gone undetected, report finds.

Why Now?

What is “Cybersecurity”?

Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks. In a computing context, security comprises **cybersecurity** and physical security -- both are used by enterprises to protect against unauthorized access to data centers and other computerized systems.

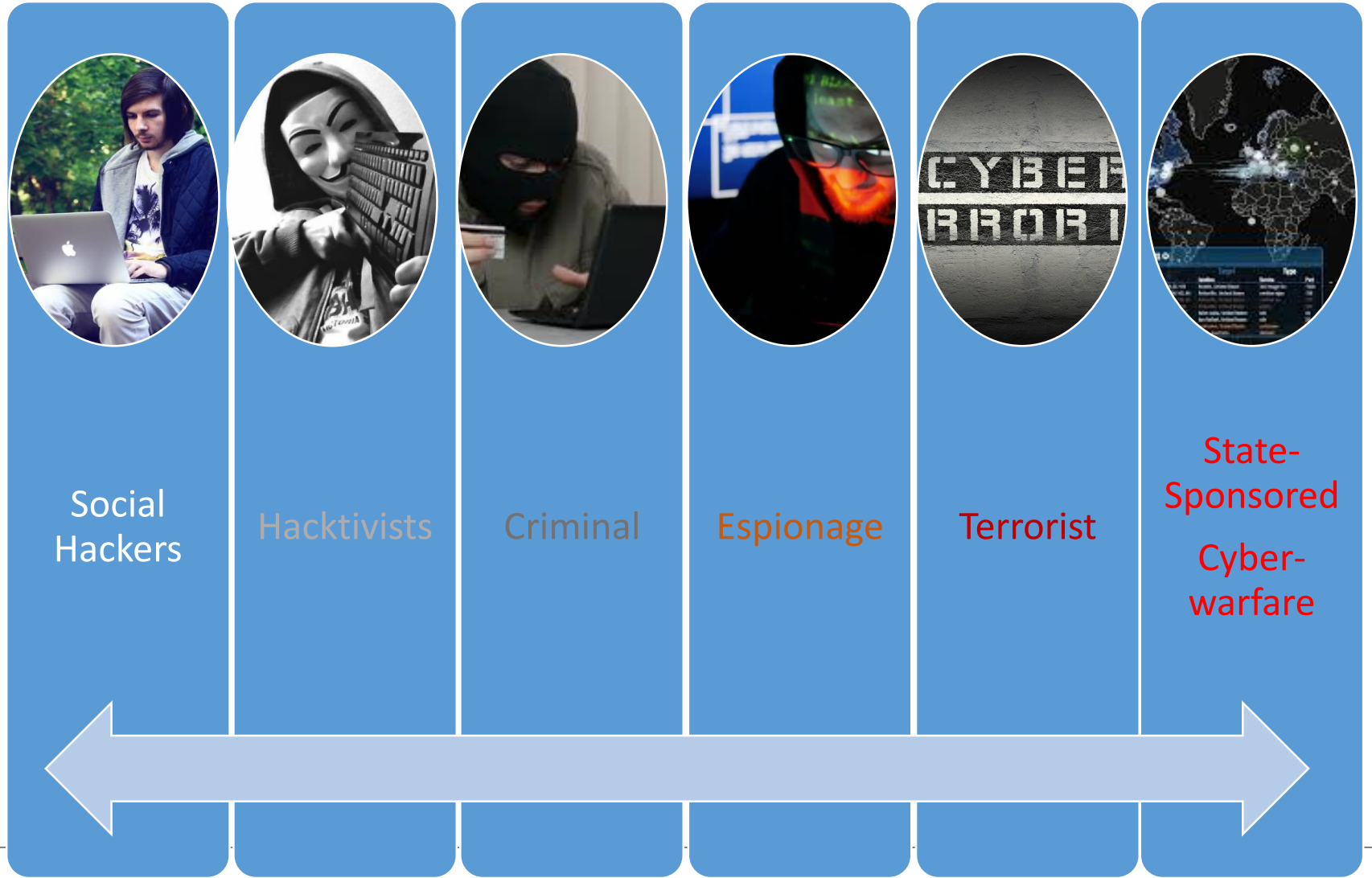


WHAT are They After?

- Destruction of Data
- Disclosure of Information
- Denial of Service
- Modification of Information
- Unauthorized Access

The cost of cybercrime could reach $6 TRILLION by 2021 (global annual cybercrime costs was estimated to be $3 trillion in 2015)

Understanding WHO is Orchestrating Cybersecurity Attacks

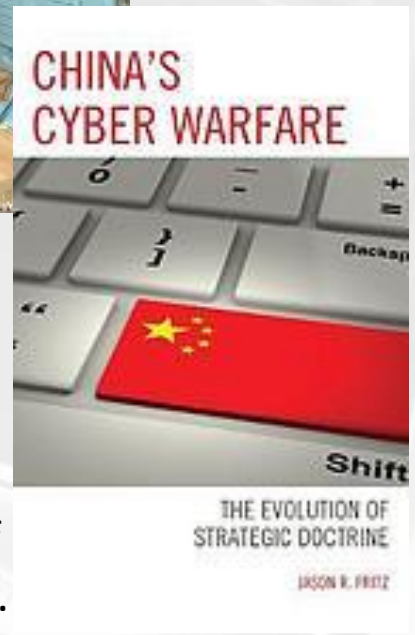


WHICH IS BIGGER?

United States Marine Corps

End of FY 2018 – Authorized Strength of 185,000 Active Personnel

China's Cyber Warriors



"State-sponsored cyber espionage is ubiquitous, with more than 100 countries actively hacking the systems of other countries and businesses. **China alone has developed an army of 180,000 cyber spies and warriors."**

Sources of Threats

- External Attacker
- Insider Threat
- Supply Chain Risk

Threat Vectors

- Phishing
- Spear Phishing
- Spoofing
- Social Engineering
- Ransomware
- Removable Media
- Insider Threats
- Negligent Users

Threat Concerns: Core Questions

- What is the potential loss from a successful attack?
- What is the likelihood of an attack?
- What is our tolerance for such a loss?
- What is our strategy to mitigate or manage this loss?
- What is our potential to recover from this breach or loss?

Protecting our Data

MARYLAND MEP
MANUFACTURING • EXTENSION • PARTNERSHIP

Maryland
DEPARTMENT OF COMMERCE

NIST Special Publication 800-171 Rev 1

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

December 2016

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

NIST 800-171 – Compliance

All Department of Defense (DoD) contractors that process, store or transmit Controlled Unclassified Information (CUI) must meet the Defense Federal Acquisition Regulation Supplement (DFARS) minimum security standards or risk losing their DoD contracts.

Examples of CUI

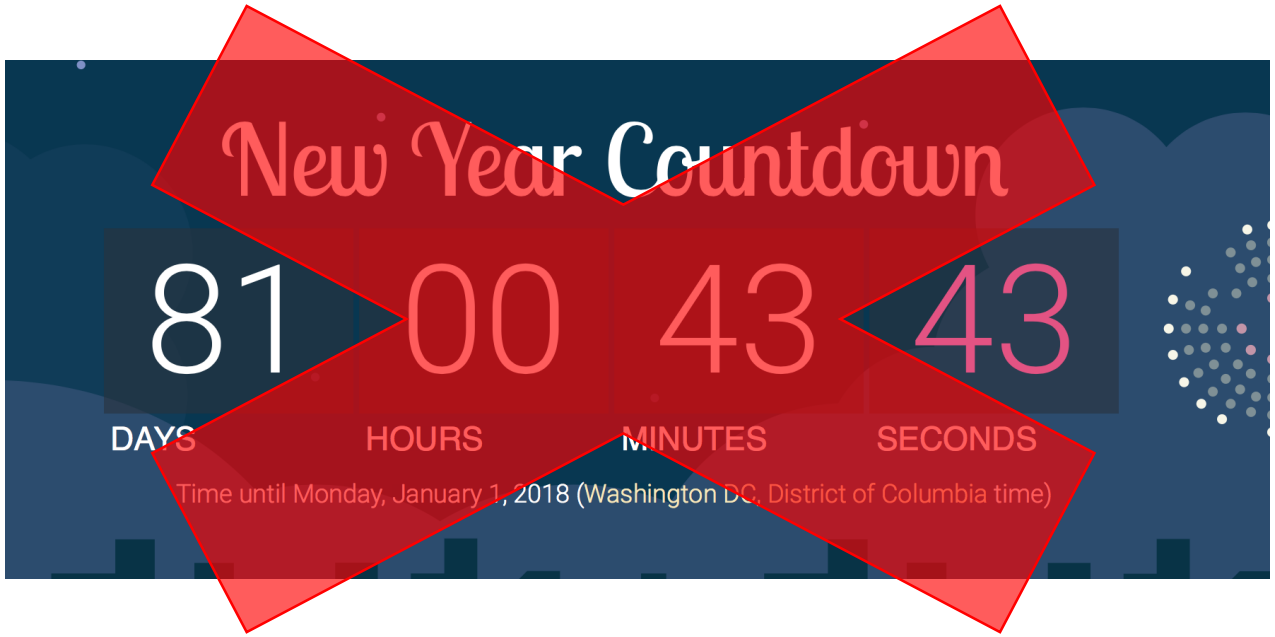
- Email
- Electronic files
- Blueprints / drawings
- Proprietary contractor / company information
- Pricing data
- Physical records

Who Needs to Comply?

- Do you deal with government controlled unclassified information?
- Typical entities: universities, research institutions, consultants, manufacturers
- Manufacturers who are prime or subcontractors to the DoD or other agencies
- Contractors OR Subcontractors who work directly with DoD or Prime contractors to support the DoD mission

When do you need to comply?

- December 31, 2017: Defense Contractors must be in compliance with NIST 800-171
  - Prime or Subcontractors



> 1 Year

Cybersecurity Compliance
The REALITY

Timeline for Implementation of The Standard

- 2016: Early Adopters and Large OEMs work towards compliance
- 2016 and 2017: DOD and Partner led Education Efforts
- Summer 2017: Compliance Language begins to appear in contract renewals and procurements
- Fall 2017: Large OEMS request compliance of subcontractors
- December 31, 2017: Deadline for Compliance

The Reality

- OEMs and Large Prime Contractors Actively Working on Compliance (Lockheed, Northrop, Textron, etc.)
- Second and Third Tier Suppliers
  - Many NOT AWARE of the Standard or Requirement
  - Many are IGNORING the Requirements
  - Many lack RESOURCES to Comply
- The Large Majority of Contractors are NOT Currently Compliant

What is NIST 800-171

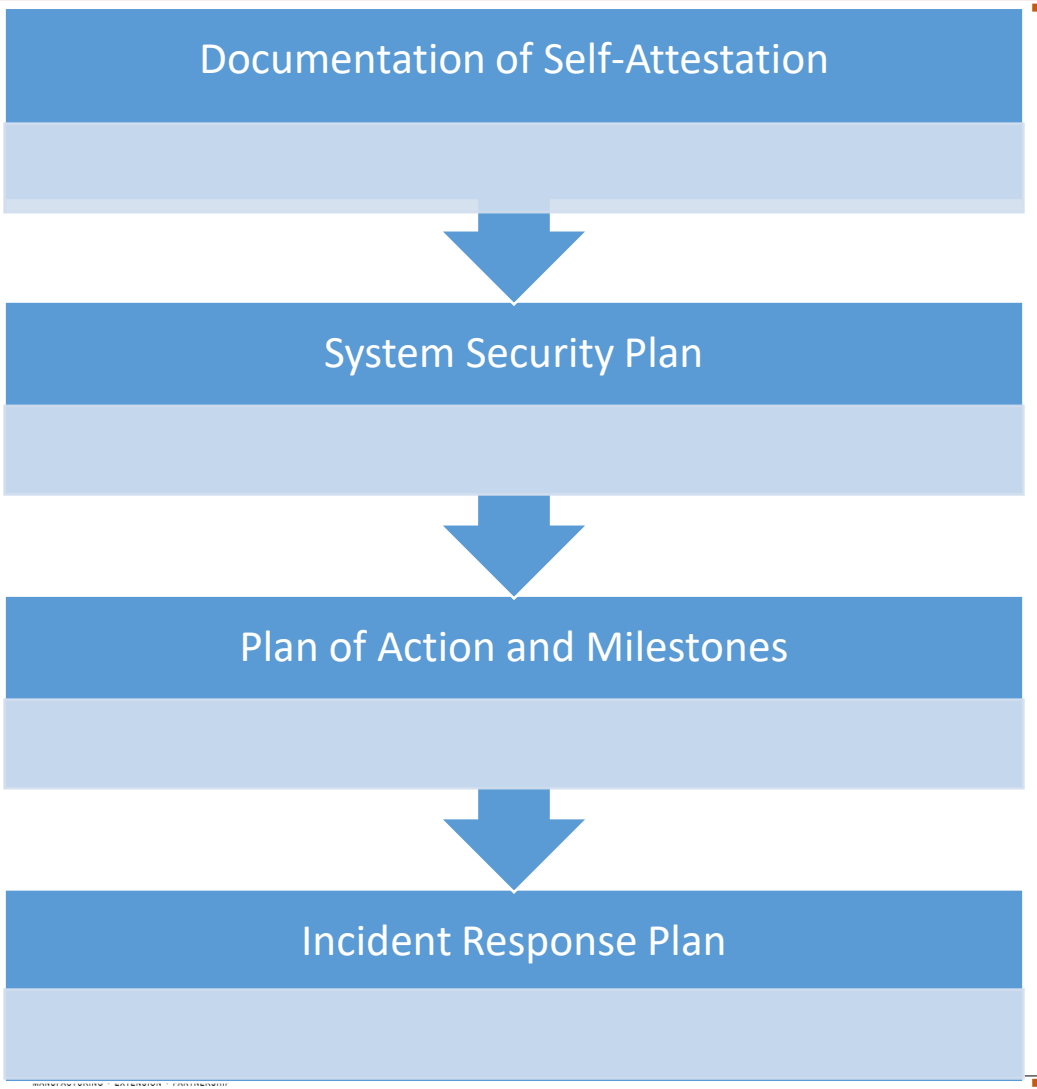
MARYLAND MEP
MANUFACTURING • EXTENSION • PARTNERSHIP

Maryland
DEPARTMENT OF COMMERCE

What is the Standard

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

“Compliance” With DFARS and 800-171
(The 4 Deliverables)



What needs to be protected

Cybersecurity level of effort

Cybersecurity Controls

4 Compliance Deliverables

DCMA Guidance

Threat Briefing

Strategic Alignment → Different Implementation Strategies → Competitive Advantage

Understanding the Requirements

- The Standard is Complex
- The Standard may be HARD to Understand and Comply With
- “Compliance” is not always a black or white issue
- The Standard is not always scalable
  - Struggle for extremely small companies
  - Struggle for non-traditional environments (production)
- Compliance can be costly … and a cost item for the company

Cybersecurity Assistance

MARYLAND MEP
MANUFACTURING • EXTENSION • PARTNERSHIP

Maryland
DEPARTMENT OF COMMERCE

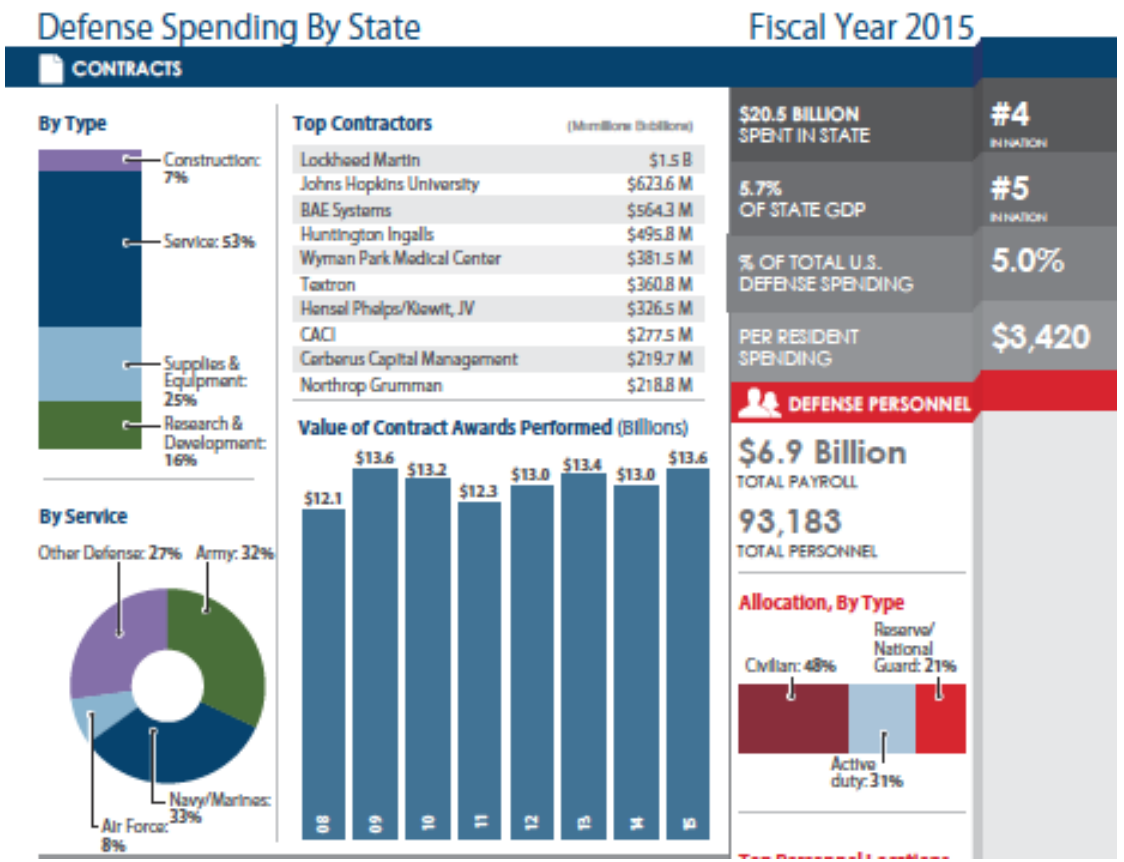
Office of Economic Adjustment (OEA)

Organization tasked with helping communities adapt to DoD program changes, expansions, cutbacks and incompatibilities between military operations and local development.

- In early 2018 Approached MD MEP to provide funding to support compliance with cybersecurity
- Able to leverage existing relationships, partnerships and programs with the Maryland Department of Commerce
- July 1, 2018 – Project funding for cybersecurity compliance for Maryland defense contractors

Why Maryland

- Defense Spending 5.7% of Maryland's GDP
- 6 of the Top 10 Defense Contractors are Manufacturers
- Hundreds of Tier 2 and Tier 3 Suppliers
- MD MEP Part of Initial Pilot for Cybersecurity for Manufacturing and 800-171 Compliance



CYBERSECURITY ASSOCIATION OF MARYLAND, INC.

MARYLAND MEP
MANUFACTURING • EXTENSION • PARTNERSHIP

Maryland
DEPARTMENT OF COMMERCE

Maryland Defense Cybersecurity Assistance Program – Program Built on Partnership

Maryland Defense Cybersecurity Assistance Program (DCAP)

- Program designed to provide education, technical assistance and resources for defense contractors in Maryland
- Program administered by Maryland Department of Commerce and MD MEP
- Program Goals:
  - Strengthen Maryland's Defense Supply Chain
  - Provide Resources for Compliance with NIST 800-171 Standard and DFARS Requirements

The Customer / Participation Requirements

- Maryland-based Defense Contractors
  - MUST have a physical location in Maryland
  - Able to demonstrate either;
    - 10% or more DoD related business
    - Contract or procurement request for compliance
- Target Audience:
  - Small and mid-sized defense contractors seeking assistance with cybersecurity requirements

Program Components

- Education
- Application
- Assessment
- Technical Assistance
- Knowledge Sharing, Training and Best Practices

800-171 Gap Assessment

- Participating Companies undergo an 800-171 Gap Assessment to Determine Level of Compliance
- Various Assessments Available
  - Company Size and Complexity
  - Company Capabilities (Internal Resources)
  - Scalable
- Financial Assistance to Offset Cost of Assessment
  - Levels of Financial Assistance Determined by Company Size
- All Participants will Be Measured Using the GOMA Risk Management Tool to generate a Baseline Score

Gap Assessment - Outcomes

- NIST 800-171 Compliance "Score" (% Compliance against the 110 Controls)
- Plan of Action and Milestones (POAM)
- Recommendations for Improvement / Mitigation
- Identification of Resources for Assistance

Technical Assistance

- Technical Assistance needs determined by assessment, level of compliance, and **Plan of Action and Milestones**
- Resources available to offset the cost of assistance / mitigation
  - Documentation
  - Training
  - Systems / Infrastructure improvements
  - Monitoring and technical tools
- Use of Maryland Cyber Resources
  - Benefits including Maryland tax credits
  - Local knowledge and development of local capabilities
- Funding Available to Offset Cost of Technical Assistance and Remediation
  - % Based on Company Size and Cost of Services
  - $ Cap / Company

How You Can Participate

MARYLAND MEP
MANUFACTURING • EXTENSION • PARTNERSHIP

Maryland
DEPARTMENT OF COMMERCE

Get Involved

- Take the first step
- Complete the application
- Meet a resource provider (or use your own)
- Undergo a gap assessment
- Develop a POAM
- Address weaknesses
- Monitor risks
- Celebrate success!

Why Participate

MARYLAND MEP
MANUFACTURING • EXTENSION • PARTNERSHIP

Maryland
DEPARTMENT OF COMMERCE

For Consideration

- Navy – ”Trust but Verify”
- Cyber Command – Initiating a Review of Contractor Procedures for Tier 1 Suppliers
- Contactor Audits
- Tier 1 and Tier 2 Suppliers and flow-down from Prime
- Competitive Advantage
  - New Contracts and Solicitations
  - Contractor Evaluation
  - International Business

Questions

MARYLAND MEP
MANUFACTURING • EXTENSION • PARTNERSHIP

Program Contact Information

Sara Keith, Program Manager

MD MEP

410-733-0219

skeith@mdmep.org

Mike Kelleher, Executive Director

MD MEP

410-505-4142

mkelleher@mdmep.org