Cybersecurity Forum For Manufacturers

MEP • MANUFACTURING EXTENSION PARTNERSHIP®

Pat Toth
Cybersecurity Services Manager
NIST MEP

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

December 5, 2019

NIST

- Non-regulatory agency of the U.S. Department of Commerce
- Serves as the **U.S. National Measurement Institute**
- Laboratory programs support U.S. innovation, standards development.
- Focus on metrology and standards

MPORTANT:

NIST *does not regulate U.S. cybersecurity* – rather, NIST provides neutral guidance, technical expertise, and reference materials for use by government agencies and industry organizations.

MEP National Network™

The Go-To Experts for Advancing U.S. Manufacturing

MEP Summary

MISSION

To strengthen and empower U.S. manufacturers

MEP National Network™

- MEP Center in all 50 U.S. states plus Puerto Rico.
- System-wide non-Federal staff of over 1,200 individuals in ~600 service locations assisting U.S. manufacturers.
- Contracting with >2,500 3rd party service providers

Local → National Connection

Network of Centers providing localized service to manufacturers in each State – with National reach and resources

MEP Budget & Business Model

$128M FY17 Federal Budget with Cost Share Requirements for Centers

Partnership Model

- Federal, State, Industry
- Managed by NIST at Federal level
- Well aligned with state and local economic development strategies

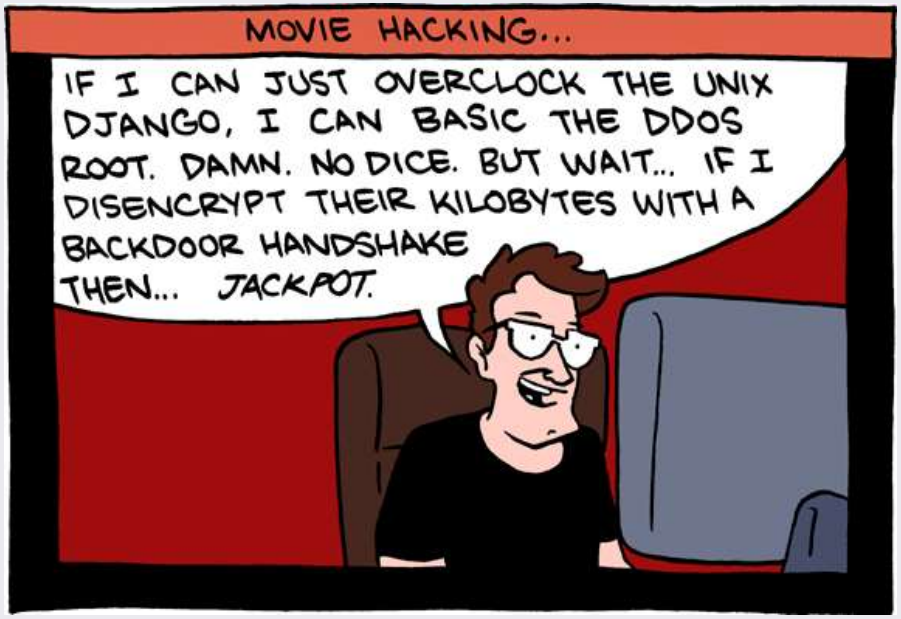
MEP Strategy: Global Competitiveness and Growth

Serve as *trusted advisors* who provide direct, hands-on technical and business assistance to America's manufacturers, striving to be the go-to resource to ensure U.S. manufacturing is resilient and leads the world in manufacturing innovation

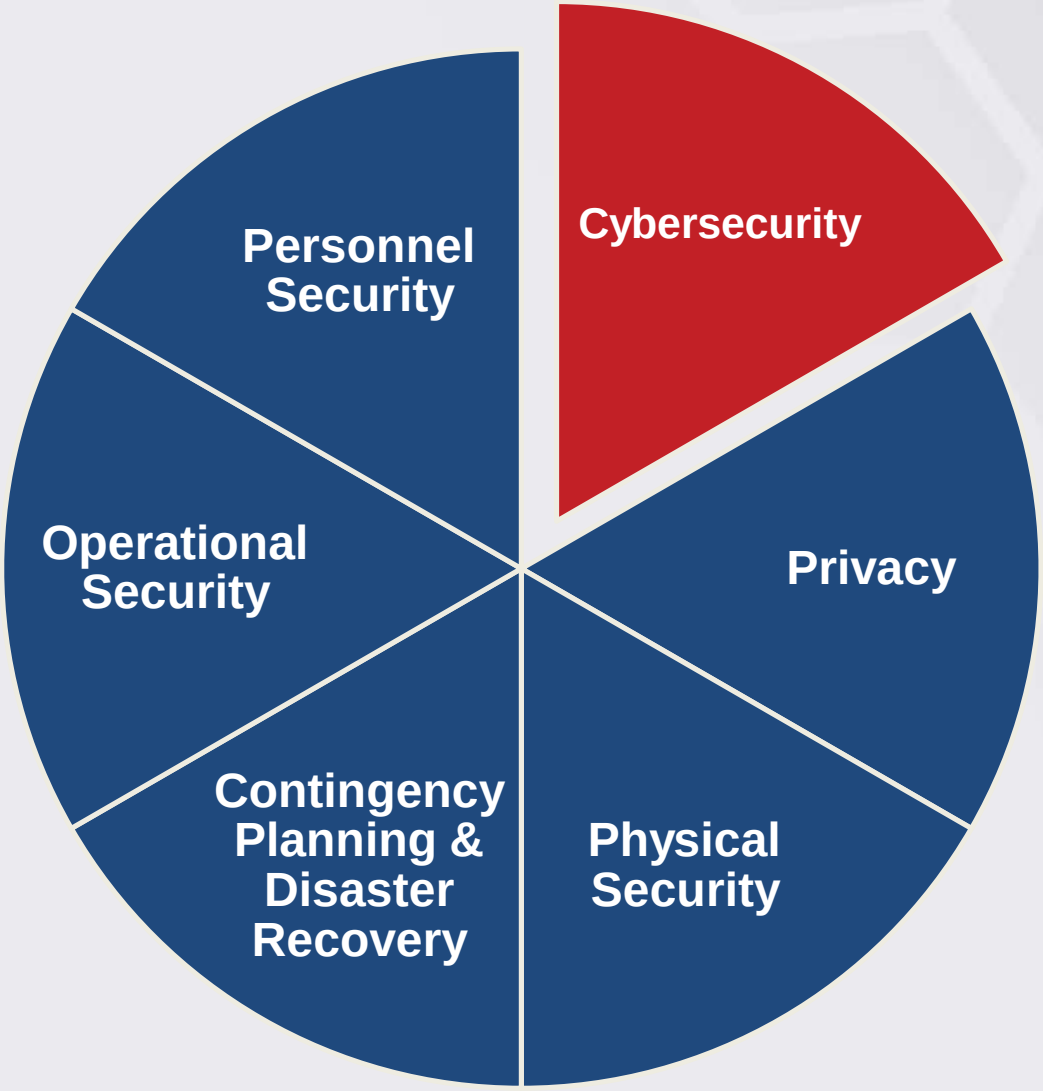
Our appetite for ***advanced technology*** is rapidly exceeding our ability to protect it.

Understanding Cybersecurity

Cybersecurity



What Is Information Security?



What Is Information Security?

Confidentiality

Unauthorized Access, Disclosure

Integrity

Unauthorized Modification, Use

Availability

Disruption, Destruction


INDUSTRY 4.0
31
SALE

Which Would YOU Go After?

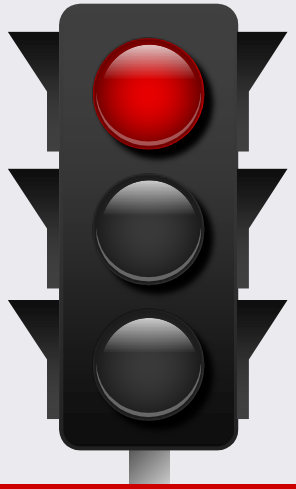
Motion and impact sensors
Video cameras
24/7/365 professionals

Simple lock
Many windows
Owners often away

Reality of Cyberattacks & Breaches

- 55% of small and mid-sized business have experienced a data breach or cyberattack
- $38,000 is the average cost for a small business to overcome a data breach
- 60% of impacted businesses are left severely impaired
- 43% of all spear-phishing attacks are targeted at small businesses

Small Business at Risk



70% of Small Businesses Not Prepared for a Cyber Attack*

Small businesses are **less likely** to have strategies in place to:

- Prevent cyber attacks
- Detect them early if they do occur
- Reduce the damage, and
- Withstand the financial impact of a hack or breach

*According to the 2018 HISCOX Small Business Cyber Risk Report

NIST Cybersecurity Framework

1 IDENTIFY

Identify and control who has access to your business information

Conduct background checks

Require individual user accounts for each employee

Create policies and procedures for cybersecurity

2 PROTECT

Limit employee access to data and information

Install Surge Protectors and Uninterruptible Power Supplies (UPS)

Patch your operating systems and applications routinely

Install and activate software and hardware firewalls on all your business networks

Secure your wireless access point and networks

Set up web and email filters

Use encryption for sensitive business information

Dispose of old computers and media safely

Train your employees

3 DETECT

Install and update anti-virus, anti-spyware, and other anti-malware programs

Maintain and monitor logs

4 RESPOND

Develop a plan for disasters and information security incidents

5 RECOVER

Make full backups of important business data and information

Continue to schedule incremental backups

Consider cyber insurance

Make improvements to processes/ procedures/ technologies

NIST Cybersecurity Framework

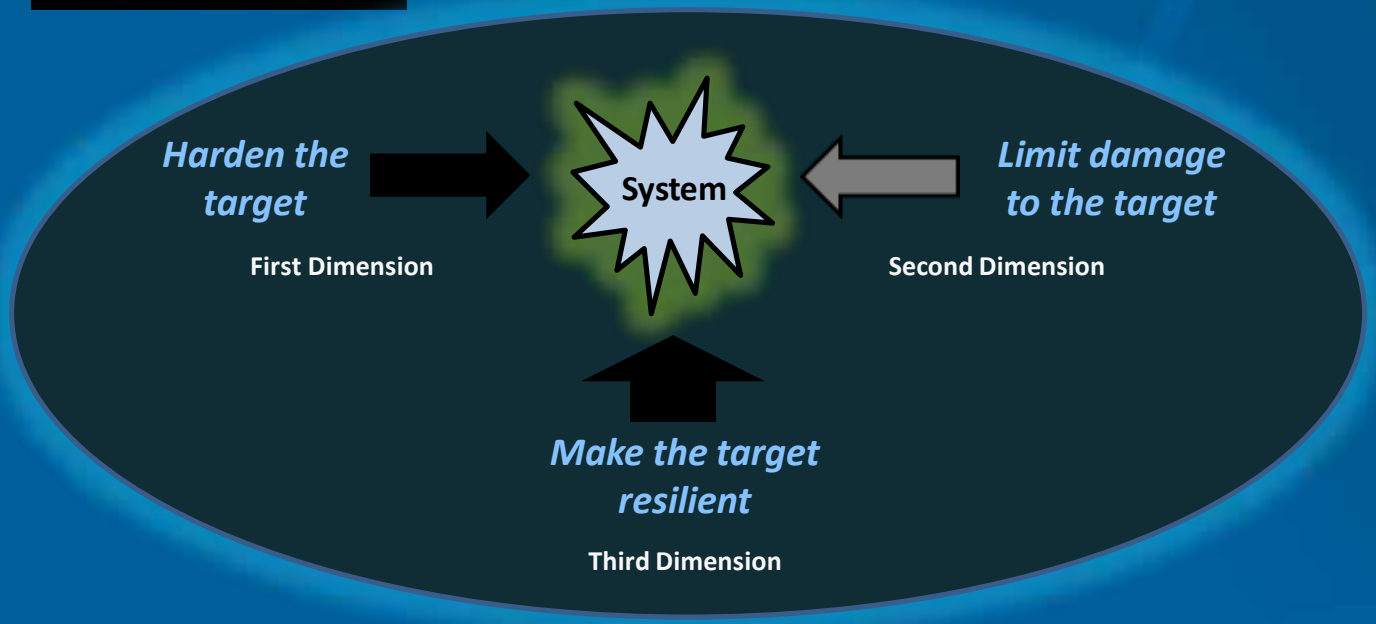
Protecting DOD Information

A Northrop Grumman X-47B (U.S.) and a Lijian Sharp Sword (China)

A Lockheed Martin F-35B Lightning II (U.S.) and a Shenyang J-31 (China)

Sea Dragon Compromise

Reducing susceptibility to ***cyber threats*** requires a multidimensional strategy.



What is the DFARS Cybersecurity Requirement?

Clause 252.204-7012 requires defense contractors and subcontractors to:

1. Provide adequate security to safeguard covered defense information (CDI) that resides on or is transiting through a contractor's internal information system or network.
2. Report cyber incidents that affect a covered contractor information system or the CDI residing therein, or that affect the contractor's ability to perform requirements designated as operationally critical support.
3. Submit malicious software discovered and isolated in connection with a reported cyber incident to the DOD Cyber Crime Center.
4. If requested, submit media and additional information to support damage assessment.
5. Flow down the clause in subcontracts for operationally critical support, or for which subcontract performance will involve CDI.

Protective measures are employed commensurate with consequences and probability of:

What is "adequate security"?

Contractors should implement, at a minimum, the security requirements in

NIST SP 800-171 rev 1 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations"

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

What is NIST SP 800-171?

- Developed by NIST to further its statutory responsibilities under Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3541 et seq., Public Law (P.L.) 113-283.

- Provides security requirements for protecting the confidentiality of CUI.

- Applies to all components of nonfederal info systems and organizations that process, store, or transmit CUI, or provide security protection for such components.

- CUI requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations. This includes DOD and is resident within DFARS clauses that apply to defense contracts.

How does a manufacturer implement SP 800-171?

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

What does this DFARS cybersecurity requirement mean?

- This requirement is an included clause in defense contracts.
- By signing a defense contract, the contractor agrees to comply with the contract terms.
- DFARS 252.204.7012 applies to info systems that process, store, or transmit **Controlled Unclassified Information (CUI).**

Controlled Unclassified Information

Supports federal missions and business functions…

…that affect the economic and national security interests of the United States.

What is Controlled Unclassified Information (CUI)?

CUI is information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls

- It replaces categories and markings such as
  - FOUO For Official Use Only
  - SBU Sensitive but Unclassified
- Examples of CUI include:
  - Controlled Technical Information,
  - Export Control Information,
  - and DoD Critical Infrastructure Security Information
- For additional information visit the National Archives CUI webpage: https://www.archives.gov/cui

What do contractors need to do to ensure compliance with DFARS and when does this apply?

- Defense contractors are required by DFARS to provide ***adequate security*** on all covered contractor info systems.
- Defense contractors must implement, at a minimum, the following information security protections:
  - NIST SP 800-171 rev 1, as soon as practical,
  - but ***not later than December 31, 2017.***

MEP 3-Step Process to Complying with DFARS Cybersecurity Requirements

- **Step 1**:
  - Develop System Security Plan
- **Step 2:**
  - Conduct Assessment
  - Produce Security Assessment Report
- **Step 3:**
  - Produce a Plan of Action

NIST SP 800-171 Security Requirements

14 Families

- 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.

NIST Handbook 162

- *"NIST MEP Self-Assessment Handbook for Assessing NIST 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements"*
- Step-by-step guide to performing a self-assessment against NIST SP 800-171
- Available at http://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf
- Downloaded over 80,000 times

Security Requirement
Awareness and Training
Example 3.2.2

Security Requirement:

Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Meeting the Requirement:

- Basic security awareness training to new employees
- Security awareness training to users when information system changes
- Annual security awareness refresher training

Security Requirement
Awareness and Training
Example 3.2.2

Security Requirement:

Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Meeting the Requirement:

- Basic security awareness training to new employees
- Security awareness training to users when information system changes
- Annual security awareness refresher training

Security Requirement
Awareness and Training
Example 3.2.2

Where to Look:

security awareness and training policy • procedures addressing security awareness training implementation • appropriate codes of federal regulations • security awareness training curriculum • security awareness training materials • security plan training records • other relevant documents or records

Who to Talk to:

employees with responsibilities for security awareness training • employees with information security responsibilities • employees with responsibilities for role-based security training • employees with assigned information system security roles and responsibilities • employees comprising the general information system user community

Perform Test On:

automated mechanisms managing security awareness training • automated mechanisms managing role-based security training


Cyber Resiliency.
The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

Cybersecurity Capability Maturity Model - CMMC

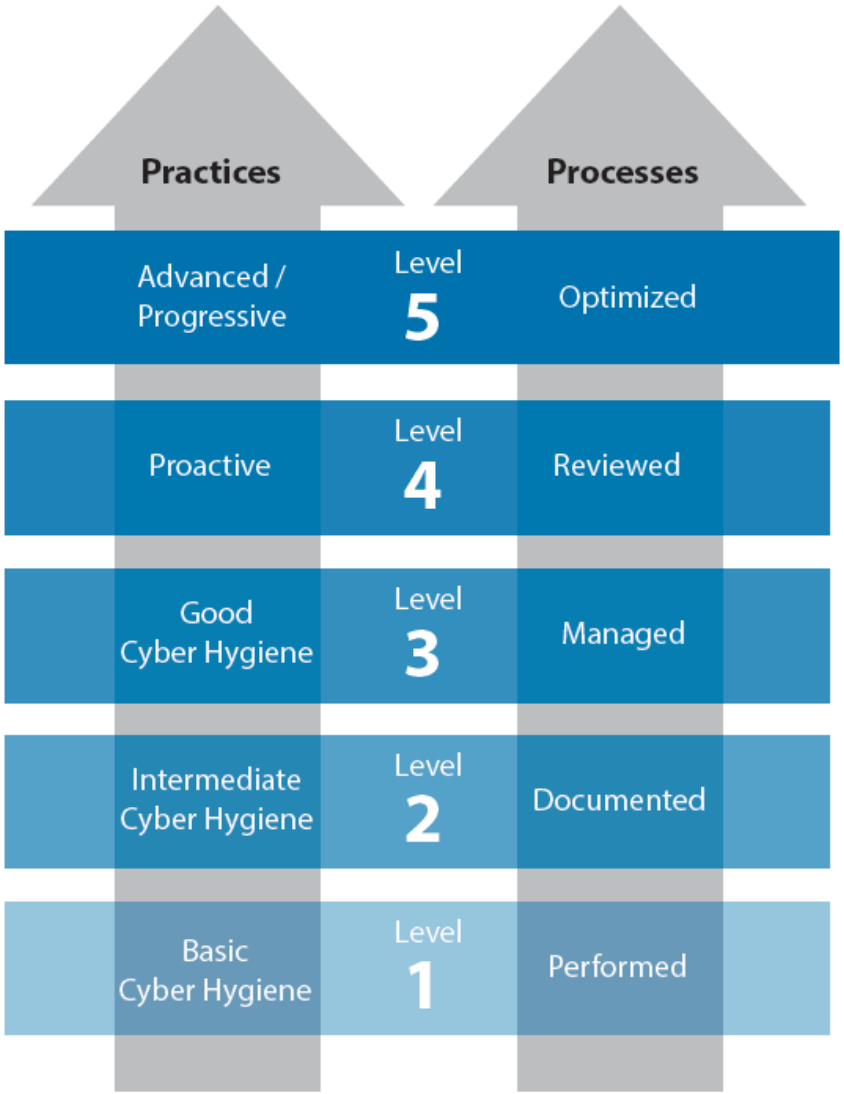
- Protect U.S. defense manufacturing supply chains.
- Incorporates the requirements from NIST SP 800-171
- Certification as cybersecurity compliant.
- Higher level, means more contracts to bid on.
- Model publication Jan 2020

https://www.acq.osd.mil/cmmc/index.html

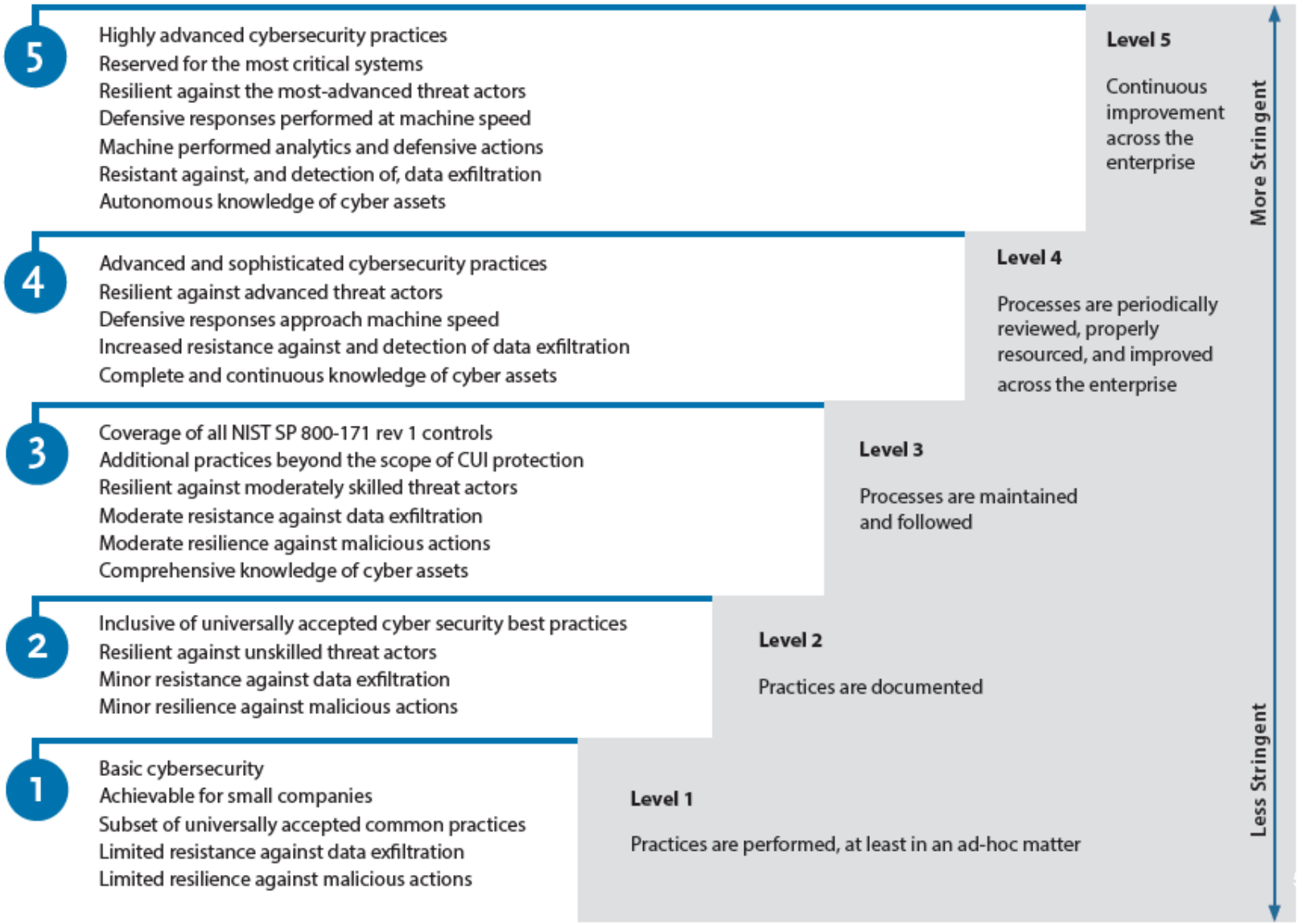
CMMC Certification

- Ranging from Level 1 “Basic Cyber Hygiene,” through Level 5 “Advanced,”
- Determined by third-party auditors.
- The CMMC level required in solicitations will be listed the solicitation’s sections L and M.
- GO/NO GO decision.
- Starting in June 2020

Capabilities Assessed for Practice & Process Maturity



CMMC Model Level Descriptions



Cyber Risk Management

- Protect Your Business
- Resiliency *NOT* Compliance

MEP National Network™

Questions?

THANK YOU!!

MEP National Network™

Pat Toth
Cybersecurity Program Manager
NIST MEP Extension Services Division
(o) 301-975-5140 (c) 240-477-3447
ptoth@nist.gov

Stay Connected

VISIT OUR BLOG!
https://www.nist.gov/blogs/manufacturing-innovation-blog

Get the latest MEP National Network news at:
www.nist.gov/mep

Contact Us:
mfg@nist.gov

301-975-5020