

Agenda

1	Why this? Why now? <ul style="list-style-type: none">- CMMC as risk-based data protection
2	What is CMMC? <ul style="list-style-type: none">- Framework- Model: structure & processes maturity- Model: maturity of cyber hygiene practices
3	Where does CMMC come from? <ul style="list-style-type: none">- Standards- Contract clauses
4	What is the timeline?
5	The Bottom Line: Expected results

Why this? Why now?

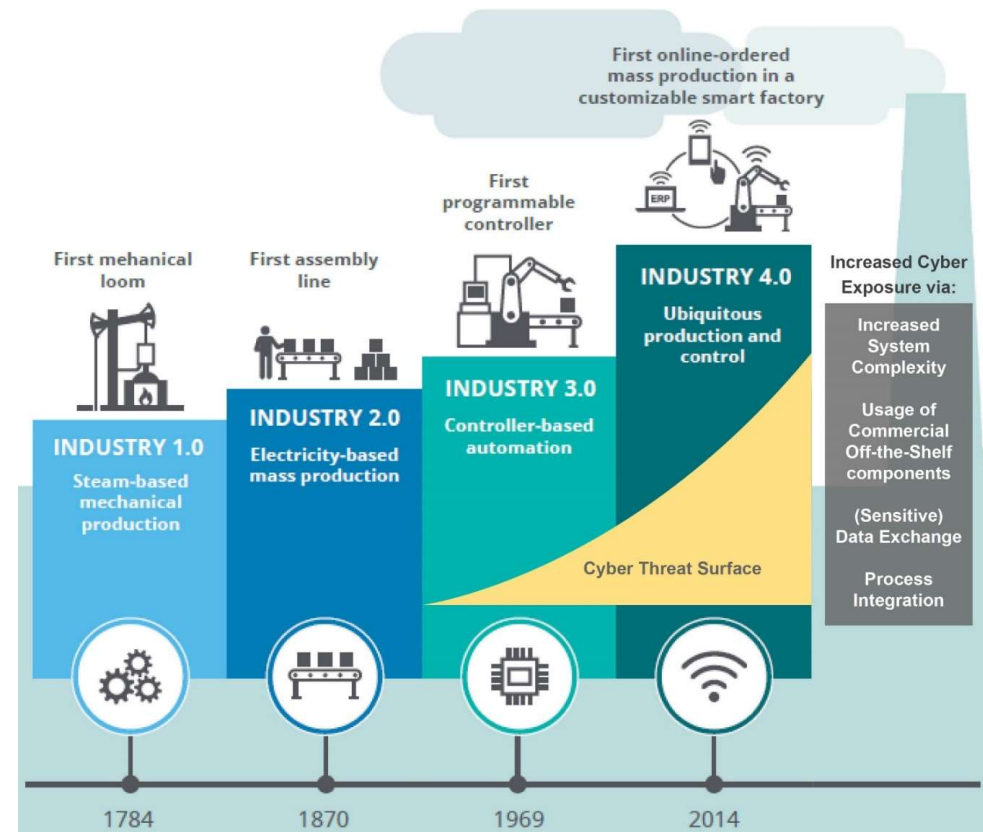
- **\$570 Billion - \$1.09 Trillion**

The estimated value of stolen intellectual property and sensitive information across all U.S. industrial sectors over 10 years

- **36-54%**

The estimated implementation of current DoD* cybersecurity requirements in place since 2013

*DoD = U.S. Department of Defense



Source: *Industry 4.0 and cybersecurity- managing risk in an age of connected production*. Deloitte.

CMMC is Risk-Based Data Protection

- CMMC is driven by the kind of data in a contract
- Federal Contract Information (FCI)
 - **“Information not intended for public release.** It is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government. FCI does not include information provided by the Government to the public.”¹
 - **Federal Acquisition Regulation (FAR) 52.204-21 specifies 15 “Basic Safeguards” equivalent to CMMC level 1**
- Controlled Unclassified Information (CUI)
 - **“Information that requires safeguarding or dissemination controls** pursuant to and consistent with applicable law, regulations, and government-wide policies **but is not classified** under Executive Order 13526 or the Atomic Energy Act”²
 - **DoD contracts with CUI specify 100 cybersecurity controls of the 130 in CMMC level 3**
- Under CMMC, each DoD contract will specify a required Maturity Level
 - Prime contractors will specify the required Maturity Level in flow down to subcontractors

Sources:

1. FAR 52.204-21

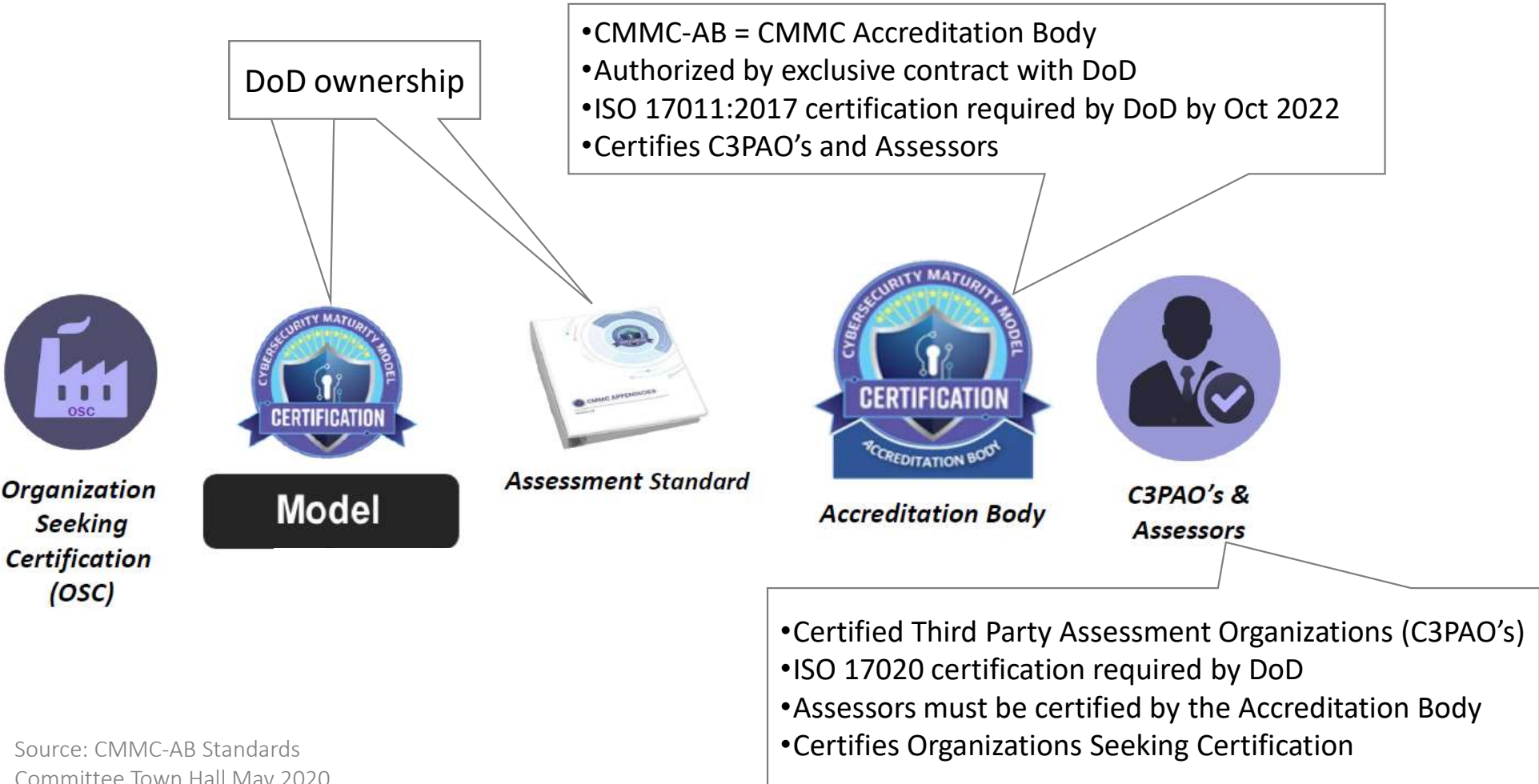
2. U.S. National Archives – About CUI

What is CMMC?

- Cybersecurity Maturity Model Certification (CMMC)
- New approach to cybersecurity requirements for contractors to the U.S. Department of Defense (DoD)

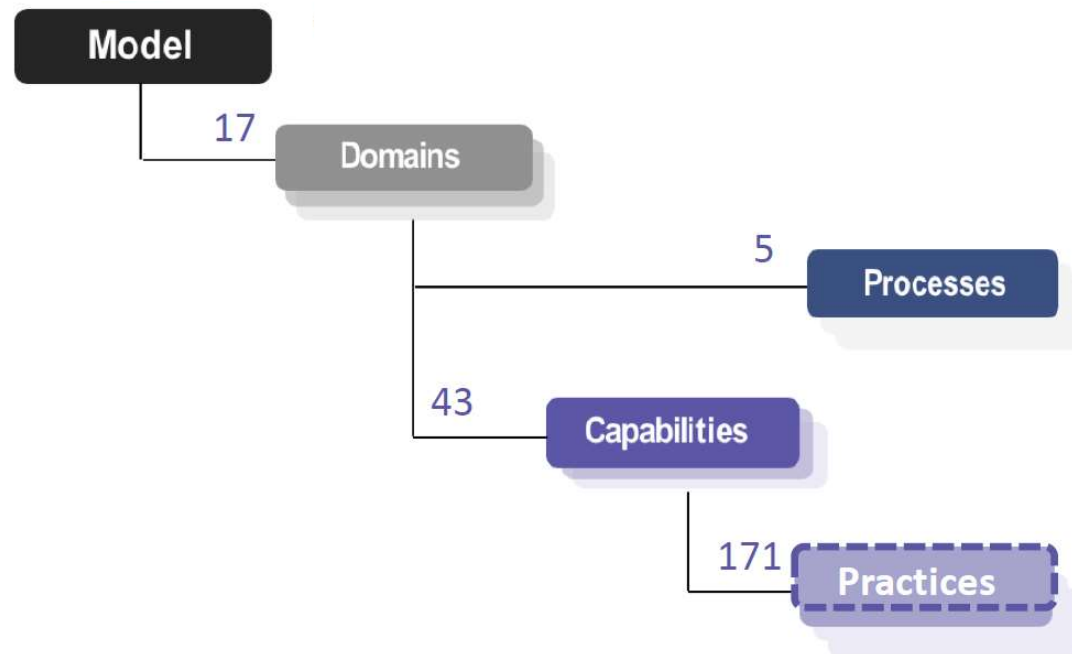
Current DoD Cybersecurity Requirements	CMMC
Based on trust	Based on trust with verification
Self-assessment	Third party assessments conducted by authorized and accredited organizations
Self-attestation of compliance at time of contract award	Certification must be complete before contract award ; three-year renewal cycle
Each company is responsible for its own compliance and to “flow down” the requirements to all of its subcontractors	The prime contractor which has the agreement directly with the DoD is responsible to ensure valid certification of all subcontractors at all tiers of the bidding team
Incomplete implementation of compliance controls may be documented on a Plan of Action with Milestones (POAM)	Compliance levels from 1 (basic) to 5 (advanced); no incomplete items allowed beyond a 90-day post assessment remediation period
Based on U.S. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171	Based on NIST SP 800-171 with selected controls added in tiers 2-5 from other respected sources
No process maturity requirement	CMMC tiers 2-5 include progressively higher requirements for process maturity

CMMC Framework



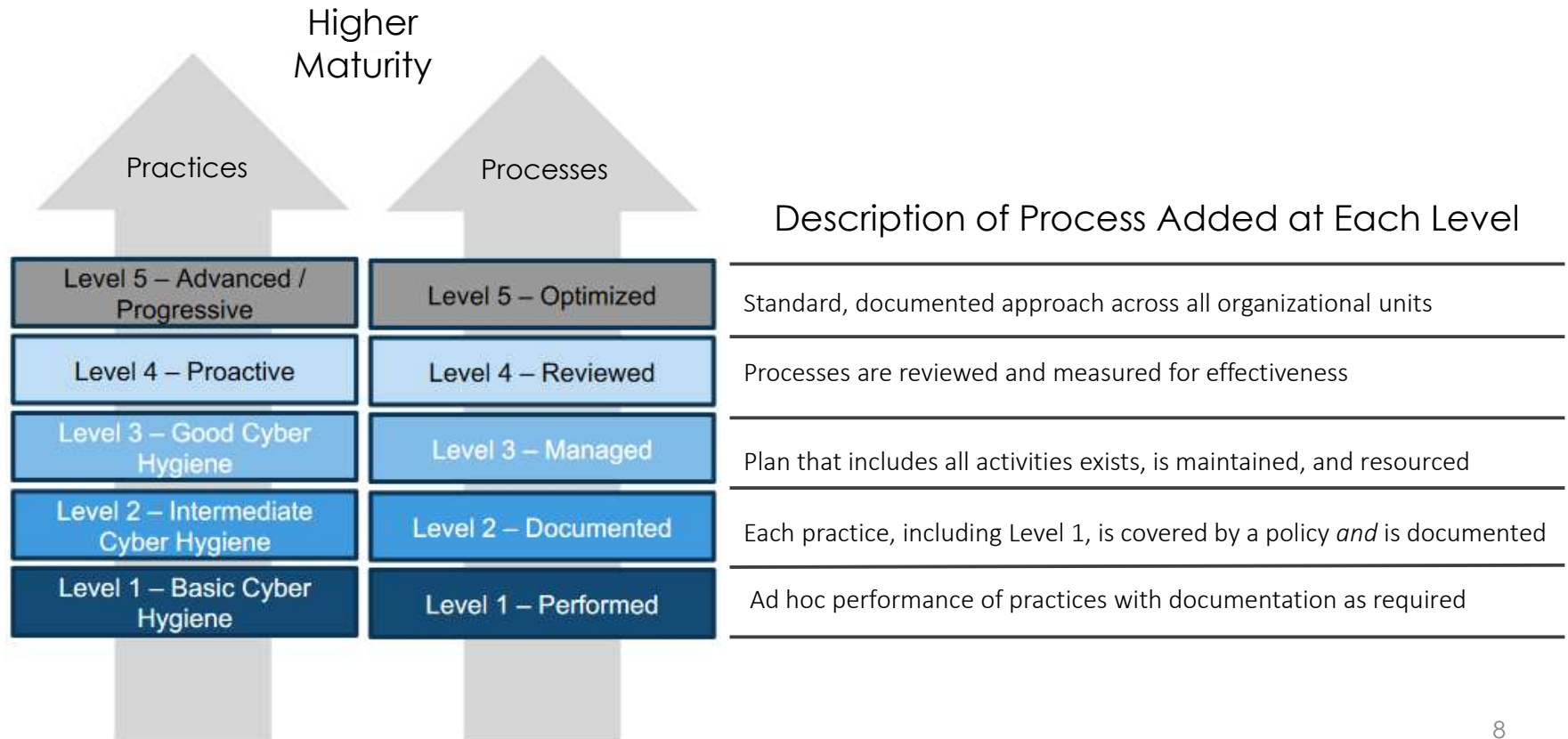
Source: CMMC-AB Standards
Committee Town Hall May 2020

CMMC Model Structure



Source: U.S. Department of Defense

CMMC Model Maturity



Source: U.S. Department of Defense

Maturity in CMMC Cyber Hygiene Practices

- Initial DoD contracts will specify only maturity level 1 (for FCI) or 3 (for CUI)
 - Levels 4 or 5 will rarely be required
 - Level 2 is progress, yet not sufficient for CUI
- Practices increase by Maturity Level
 - There is a BIG increase between levels 1 & 2
 - Another BIG increase between levels 2 & 3
- The only reason to aim for a certification higher than specified is to anticipate a future contract at that level
 - Compliance ≠ security. Some organizations do higher maturity practices for security

CMMC Level	Additional Practices Required at each CMMC Level	Maturity Level Influence on Practices	
1	17	Performed (17)	FCI
2	+55	Documented (72)	FCI
3	+58	Managed (130)	CUI/FCI
4	+26	Reviewed (156)	CUI/FCI
5	+15	Optimized (171)	CUI/FCI
Total Practices	171		

Source: CMMC-AB Standards Committee Town Hall May 2020

Where Does CMMC Come From? Mapping to Standards

CMMC Level	Additional Practices Required at each CMMC Level	Maturity Level Influence on Practices	Sources of Standards in CMMC Model		
			NIST SP 800-171r2 NIST SP 800-171A	NIST SP 800-172	Other
The CMMC Assessment Standard					
1	17	Performed (17)	17	–	–
2	+55	Documented (72)	48	–	7
3	+58	Managed (130)	110	–	20
4	+26	Reviewed (156)	110	11	35
5	+15	Optimized (171)	110	15	46
Total Practices	171		110	15	46

Other standards

- U.K National Cyber Security Centre (NCSC) Cyber Essentials
- Australian Cyber Security Centre (ACSC) Essential Eight
- Center for Internet Security (CIS) Controls
- Cybersecurity Framework (CSF)

Acronyms

- CFR** = Code of Federal Regulations
NIST = National Institute of Standards and Technology
SP = Special Publication

Source: CMMC-AB Standards Committee Town Hall May 2020

Mapping Current DoD Contract Clauses to Standards & CMMC

•DFARS 252.204-7021 contains CMMC requirements

- Additional acronyms**
- CFR = Code of Federal Regulations
 - DFARS = Defense Federal Acquisition Regulations Supplement
 - FAR = Federal Acquisition Regulations (note: 48 CFR = FAR)
 - PMO = Program Management Office

CMMC Level	Additional Practices Required at each CMMC Level	Maturity Level Influence on Practices	Sources of Requirements in CMMC Model			
			48 CFR 52.204-21 FAR 52.204-21	32 CFR 2002 DFARS 252.204-7012 DFARS 252.204-7008 DFARS 252.204-7009 Other	DoD CMMC PMO	DoD CMMC PMO
			Sources of Standards in CMMC Model			
			*Note: 15 safeguarding requirements from 48CFR 52.204-21 correspond to 17 security requirements in NIST SP 800-171	NIST SP 800-171r2 NIST SP 800-171A	NIST SP 800-172	Other
The CMMC Assessment Standard						
1	17	Performed (17)	15*	17*	-	-
2	+55	Documented (72)	-	48	-	7
3	+58	Managed (130)	-	110	-	20
4	+26	Reviewed (156)	-	110	11	35
5	+15	Optimized (171)	-	110	15	46
Total Practices	171			110	15	46

Source: CMMC-AB Standards Committee Town Hall May 2020

Timeline: What's Required Now?

- Self-assessment and self-attestation
- 48 CFR 52.204-21 applies to **all current DoD contractors**
 - 15 Basic Safeguards for FCI **comparable to CMMC level 1**
 - Includes requirement to flow down to sub-contractors
- Contracts with DFARS 252.204-7008 or -7012 require **compliance with NIST SP 800-171 for CUI**
 - This covers **110 of the 130 practices in CMMC level 3**
- DFARS 252.204-7012 is required in **all new DoD contracts with CUI**
 - Includes requirement to flow down to sub-contractors
- Interim Rule for **all new contracts & extensions with CUI**
 - DFARS 252.204-7019 and 7020 effective November 30, 2020
 - Compliance assessment not more than 3 years old must be on record in SPRS
 - Provides for assessments at low (self-assessment), medium and high (DCMA) confidence
 - Contractor must provide Government access to facilities and systems for medium and high assessments
 - Contractor must ensure sub-contractors report assessments in SPRS

Regulation	Compliance deadline
48 CFR 52.204-21 = FAR 52.204-21	October 2016
Contract Clause	
DFARS 252.204-7008	October 2016
DFARS 252.204-7012	December 2017
DFARS 252.204-7019	November 2020
DFARS 252.204-7020	November 2020

New Acronyms

DCMA = Defense Contract Management Agency

SPRS = Supplier Performance Risk System

When does CMMC begin?

- Clause DFARS 252.204-7021 will be included slowly at first
 - Requires approval by the DoD Chief Information Security Officer for Acquisition and Sustainment
- 15 selected contracts were expected starting Fiscal Year 2021
 - Each contract includes the entire bidding team with all sub-contractors
 - As of April, fewer than 10 have been announced and two have been delayed
- Entire Defense Industrial Base (DIB) to be included by Fiscal Year 2026 (Oct. 1, 2025)
 - Applies to DoD contracts with international organizations and international locations
 - Applies to universities and other DoD funded research centers
 - Estimated to include 300,000 organizations
- Civilian Agencies are exploring CMMC
 - Government Services Administration (GSA)
 - Department of Homeland Security (DHS)

Total Number of New Prime Contracts Awarded Each Year with CMMC Requirement					
	FY21	FY22	FY23	FY24	FY25
	15	75	250	479	479
Total Number of Prime Contractors and Sub-Contractors with CMMC Requirement					
	FY21	FY22	FY23	FY24	FY25
Total	1,500	7,500	25,000	47,905	47,905

Source: U.S. Department of Defense

The Bottom Line: Expected Results



Level	Scope	Expected Results
1	<ul style="list-style-type: none"> • Basic cybersecurity • Subset of universally accepted common practices 	<ul style="list-style-type: none"> • Achievable for small companies • Limited resistance to data exfiltration • Limited resilience against malicious actions
2	<ul style="list-style-type: none"> • Includes universally accepted cybersecurity best practices 	<ul style="list-style-type: none"> • Resilience against unskilled threat actors • Minor resistance to data exfiltration • Minor resilience against malicious actions
3	<ul style="list-style-type: none"> • Includes all current CUI protections and additional practices • Comprehensive knowledge of cyber assets 	<ul style="list-style-type: none"> • Resilient against moderately threat actors • Moderate resistance to data exfiltration • Moderate resilience against malicious actions
4	<ul style="list-style-type: none"> • Advanced and sophisticated cybersecurity practices • Complete and continuous knowledge of cyber assets 	<ul style="list-style-type: none"> • Resilient against advanced skilled threat actors • Increased resistance against and detection of data exfiltration • Defensive responses approach machine speed
5	<ul style="list-style-type: none"> • Highly advanced cybersecurity practices • Reserved for the most critical systems • Autonomous knowledge of cyber assets 	<ul style="list-style-type: none"> • Resilient against most advanced skilled threat actors • Resistant against, and detection of, data exfiltration • Defensive responses performed at machine speed

Source: U.S. Department of Defense

Thank you for your attention!

Linda.Rust@SecuriThink.com



Thank you for your attention!
Thanks to Debra Hampton for the invitation

Happy to take questions or have discussion at:
Linda.Rust @ SecuriThink.com

- Connect on LinkedIn
- Also see the CMMC article in PECB Insights issue 30