# Department of Defense's Cybersecurity Maturity Model Certification (CMMC)

**Presented by:**
**John D Nell**
**President, NELL 360 Solutions**
**619.709.1092**
**John.nell@ns360solutions.com**

# John Nell

A retired Navy Captain of 26 years with combat tours in Desert Storm (1991), Iraqi Freedom (2003) and Enduring Freedom – Afghanistan (2009-2010). John's highlighted tours included a frigate (USS UNDERWOOD), the Pentagon, an aircraft carrier (USS NIMITZ), Navy Recruiting, and the responsibility for manning of the Naval Air Forces. He received a Bronze Star for serving as the Senior Advisor to the Afghanistan Minister of Interior.

In 2014, John retired from the Navy and entered the civilian life as a consultant to the Department of Defense (DoD) working with NAVWAR (formally SPAWAR), the Navy and the Air Force. Companies he worked for were Booz Allen Hamilton, Omni2Max and Trabus Technologies.

Founded NELL 360 Solutions, a consulting services firm that advises companies how to effectively do business with the government, particularly the Department of Defense (DoD). Specifically, NELL 360 Solutions provides consulting in business development, talent acquisition, project management and cybersecurity risk management, particularly compliance with the DoD's NIST SP-800-171, and the latest with the Cybersecurity Maturity Model Certification (CMMC).

A member of the National Defense Industrial Association (NDIA) Cyber Division Cyber Legal Policy Committee that works closely with DoD's CMMC team in drafting the current CMMC; this included meetings with top DoD officials in Washington DC periodically in the last year.

# Background

- Cybersecurity is a very serious threat for the defense industry, the Department of Defense and all of government.
- Both the National Security Strategy and National Defense Strategy underscore the importance of defending against cyber attacks.
- $600 billion dollars, or about 1% of GDP each year is lost through cyber theft.
- Adversaries know that in today's great power competition environment, information and technology are both key cornerstones and -- and attacking the Defense Industry is much more appealing.

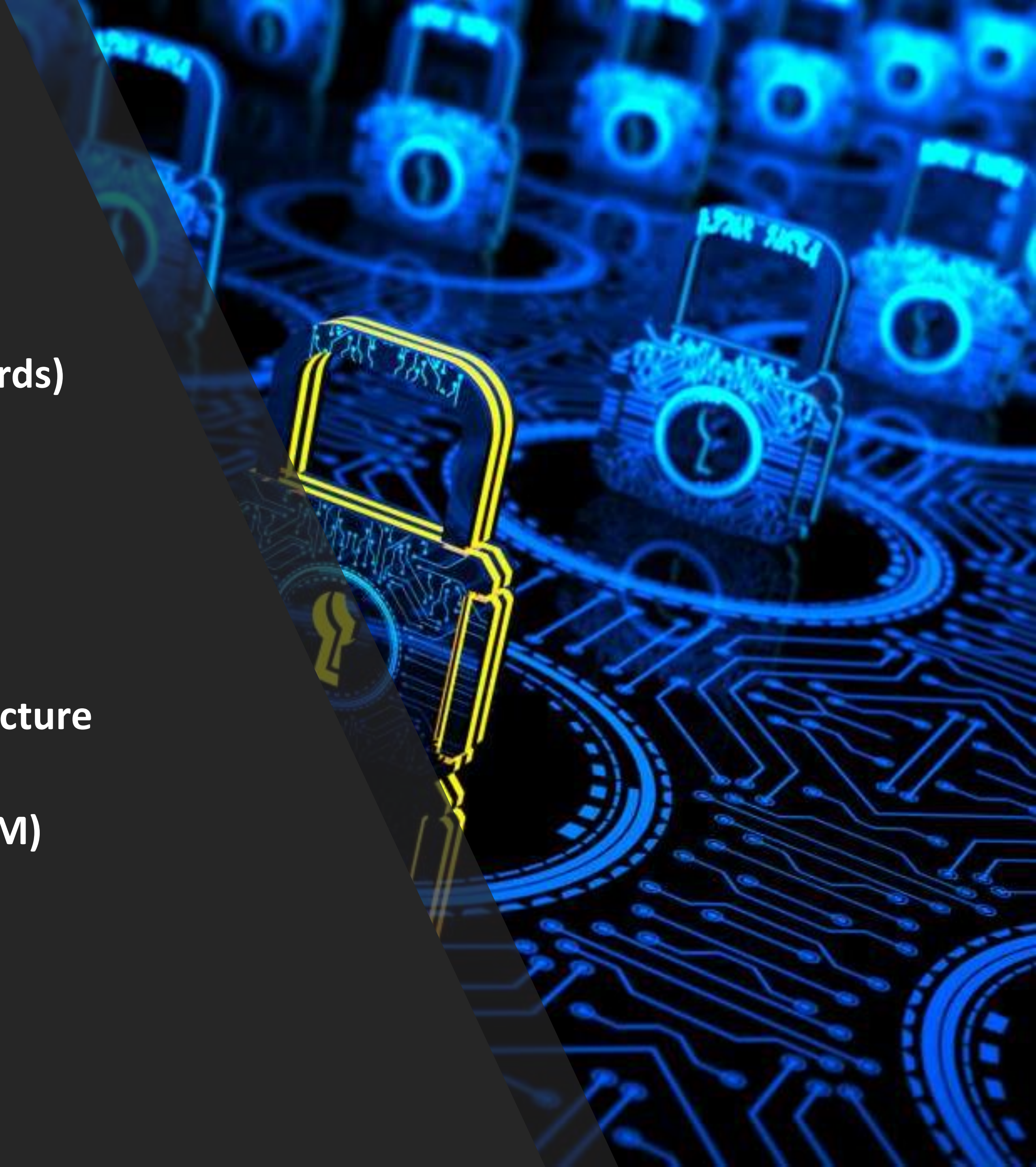
Sea Dragon – 2018 Chinese hackers had compromised the computers of a Navy contractor and stolen 614 gigabytes of data. “signals and sensor data, submarine radio room information relating to cryptographic systems, and the Navy submarine development unit’s electronic warfare library.”

# What Is Cybersecurity Maturity Model Certification (CMMC)?

- **Developed by Carnegie Mellon and the Johns Hopkins University Applied Physics Laboratory**
- **CMMC marks the first step towards implementing the new cybersecurity standards into all DoD contracts.**
- **Old Way: Under DFARS 252.204-7012, using NIST SP-800-171, contractors could self-certify – i.e., they could claim current compliance, or they could claim their intention to be compliant.**
- **New Way: Defense Suppliers must be inspected by assessors under CMMC.**
- **The model consists of five levels of security standards**
- **The CMMC will encompass multiple maturity levels that ranges from "Basic Cybersecurity Hygiene" to "Advanced".**

# Sources for the CMMC

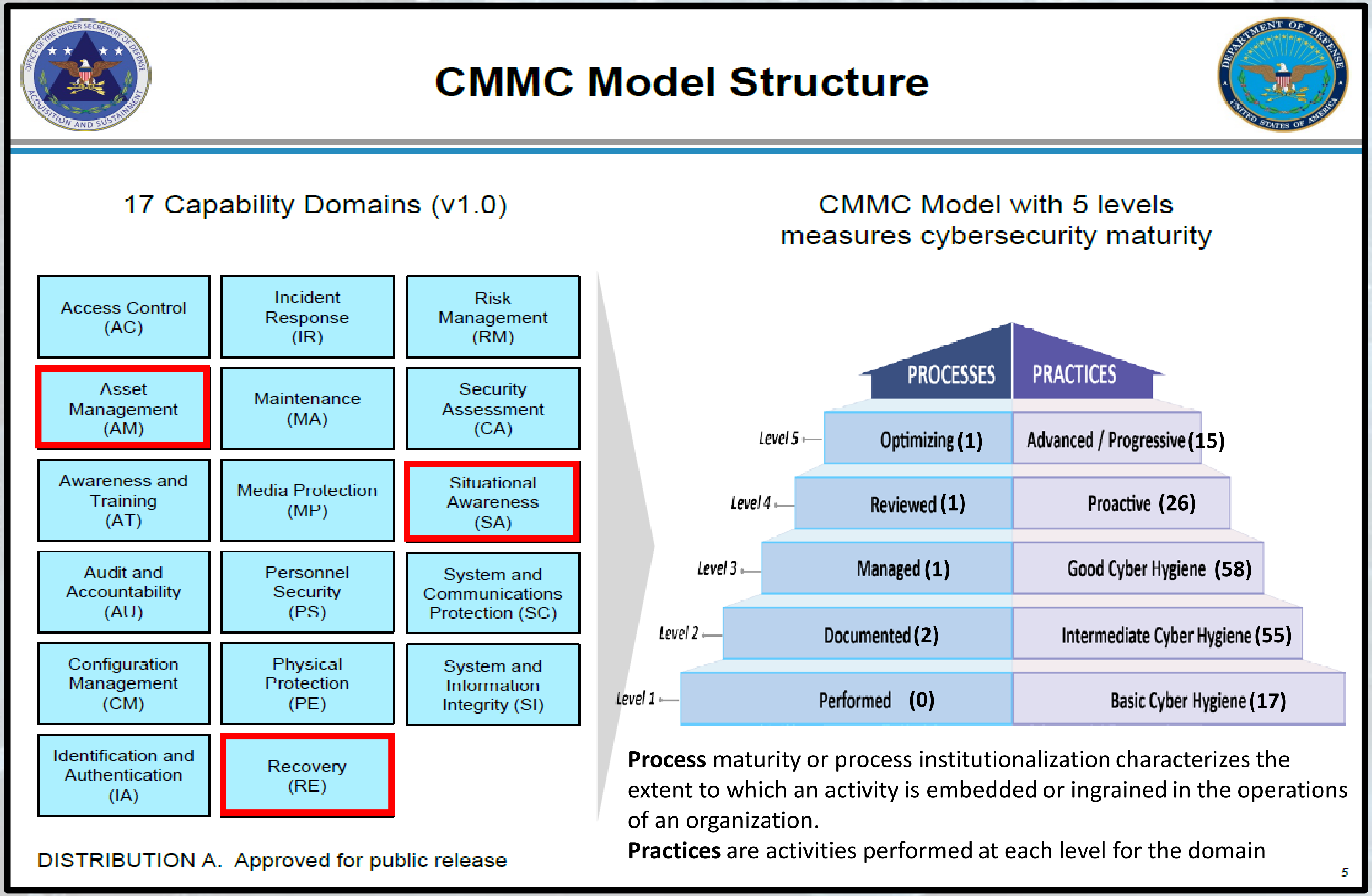
- **48 CFR 52.204-21 (Contains basic cyber safeguards)**
- **DFARS 252.204-7012**
- **NIST SP 800-171 Rev 2**
- **Draft NIST SP 800-171B**
- **CIS Controls v7.1**
- **NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF) v1.1**
- **CERT Resilience Management Model (CERT RMM) v1.2 – NIST SP 800-53 Rev 4**
- **Others such as CMMC Board, UK NCSC Cyber Essentials, or AU ACSC Essential Eight**



# What is “DoD Sensitive Information?”

- The level of CMMC you will need depends on the type of information in your IT system
- DoD sensitive (unclassified) information encompasses two major buckets:
  - Federal Control Information (FCI) – information provided by or generated for the government under contract not intended for public release
  - Controlled Unclassified Information (CUI) – information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies

# Capabilities and Maturity Levels



## CMMC Model Structure

17 Capability Domains (v1.0)

| | | |
|---|---|---|
| Access Control (AC) | Incident Response (IR) | Risk Management (RM) |
| Asset Management (AM) | Maintenance (MA) | Security Assessment (CA) |
| Awareness and Training (AT) | Media Protection (MP) | Situational Awareness (SA) |
| Audit and Accountability (AU) | Personnel Security (PS) | System and Communications Protection (SC) |
| Configuration Management (CM) | Physical Protection (PE) | System and Information Integrity (SI) |
| Identification and Authentication (IA) | Recovery (RE) | |

CMMC Model with 5 levels measures cybersecurity maturity

| | PROCESSES | PRACTICES |
|---|---|---|
| Level 5 | Optimizing (1) | Advanced / Progressive (15) |
| Level 4 | Reviewed (1) | Proactive (26) |
| Level 3 | Managed (1) | Good Cyber Hygiene (58) |
| Level 2 | Documented (2) | Intermediate Cyber Hygiene (55) |
| Level 1 | Performed (0) | Basic Cyber Hygiene (17) |

**Process** maturity or process institutionalization characterizes the extent to which an activity is embedded or ingrained in the operations of an organization.
**Practices** are activities performed at each level for the domain

DISTRIBUTION A. Approved for public release

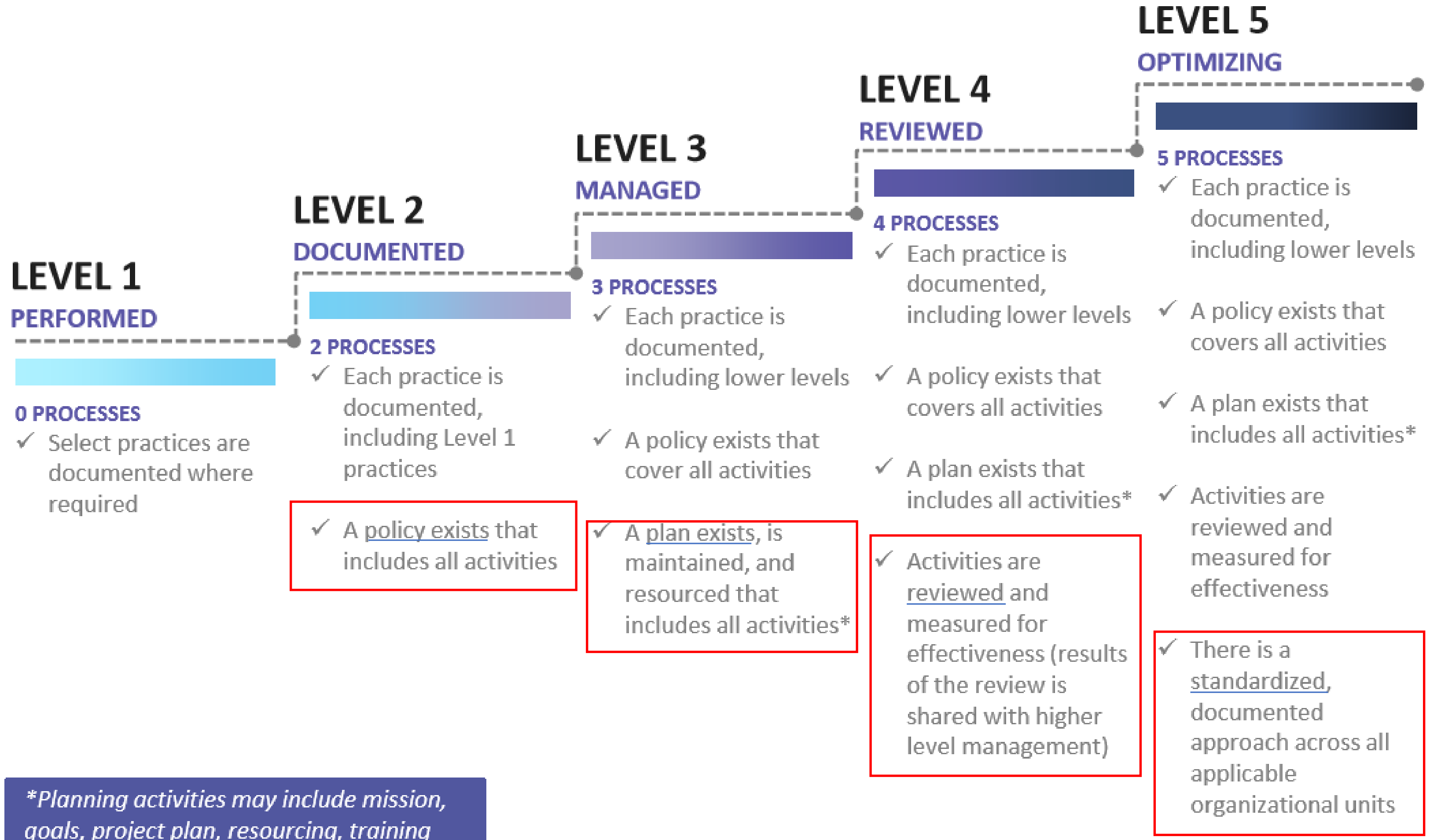
**Level 1 (Safeguard Federal Contract Information) will be focused on "basic cyber hygiene" practices such as using anti-virus software and regularly changing passwords. Basically follows FAR 52.204-21.**

**Level 2 (Transition Step to Protecting Controlled Unclassified Information (CUI)) will require "intermediate cyber hygiene" and serve as a steppingstone to Level 3.**

**Level 3 (Protect CUI) is what the Pentagon expects a plurality of the defense industrial base to achieve. NIST SP-800-171 Rev2 compliant.**

**Standards for Levels 4 and 5 (Protect CUI / Reduce Risk of Advance Persistent Threats (APT))are even more stringent and will be imposed on "very critical technology companies" working with the most sensitive information.**

# CMMC Maturity Process Progression



## LEVEL 1
**PERFORMED**

**0 PROCESSES**

- ✓ Select practices are documented where required

## LEVEL 2
**DOCUMENTED**

**2 PROCESSES**

- ✓ Each practice is documented, including Level 1 practices
- ✓ A policy exists that includes all activities

## LEVEL 3
**MANAGED**

**3 PROCESSES**

- ✓ Each practice is documented, including lower levels
- ✓ A policy exists that cover all activities
- ✓ A plan exists, is maintained, and resourced that includes all activities*

## LEVEL 4
**REVIEWED**

**4 PROCESSES**

- ✓ Each practice is documented, including lower levels
- ✓ A policy exists that covers all activities
- ✓ A plan exists that includes all activities*
- ✓ Activities are reviewed and measured for effectiveness (results of the review is shared with higher level management)

## LEVEL 5
**OPTIMIZING**

**5 PROCESSES**

- ✓ Each practice is documented, including lower levels
- ✓ A policy exists that covers all activities
- ✓ A plan exists that includes all activities*
- ✓ Activities are reviewed and measured for effectiveness
- ✓ There is a standardized, documented approach across all applicable organizational units

**Planning activities may include mission, goals, project plan, resourcing, training needed, and involvement of relevant stakeholders*

DISTRIBUTION A. Approved for public release

# CMMC Practices

| Access Control (AC) | Asset Management (AM) | Audit & Accountability (AU) | Awareness & Training (AT) | Configuration Management (CM) | Identification & Authentication (IA) | Incident Response (IR) | Maintenance (MA) | Media Protection (MP) | Personnel Security (PS) | Physical Protection (PE) | Recovery (RE) | Risk Management (RM) | Security Assessment (CA) | Situational Awareness (SA) | Systems & Communication Protection (SC) | System & Information Integrity (SI) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AC.1.001 | AM.3.036 | AU.2.041 | AT.2.056 | CM.2.061 | IA.1.076 | IR.2.092 | MA.2.111 | MP.1.118 | PS.2.127 | PE.1.131 | RE.2.137 | RM.2.141 | CA.2.157 | SA.3.169 | SC.1.175 | SI.1.210 |
| AC.1.002 | AM.4.226 | AU.2.042 | AT.2.057 | CM.2.062 | IA.1.077 | IR.2.093 | MA.2.112 | MP.2.119 | PS.2.128 | PE.1.132 | RE.2.138 | RM.2.142 | CA.2.158 | SA.4.171 | SC.1.176 | SI.1.211 |
| AC.1.003 | 1% | AU.2.043 | AT.3.058 | CM.2.063 | IA.2.078 | IR.2.094 | MA.2.113 | MP.2.120 | 1% | PE.1.133 | RE.3.139 | RM.2.143 | CA.2.159 | SA.4.173 | SC.2.178 | SI.1.212 |
| AC.1.004 |  | AU.2.044 | AT.4.059 | CM.2.064 | IA.2.079 | IR.2.096 | MA.2.114 | MP.2.121 |  | PE.1.134 | RE.5.140 | RM.3.144 | CA.3.163 | 2% | SC.2.179 | SI.1.213 |
| AC.2.005 |  | AU.3.045 | AT.4.060 | CM.2.065 | IA.2.080 | IR.2.097 | MA.3.115 | MP.3.122 |  | PE.2.135 | 2% | RM.3.146 | CA.3.164 |  | SC.3.177 | SI.2.214 |
| AC.2.006 |  | AU.3.046 | 3% | CM.2.066 | IA.2.081 | IR.3.098 | MA.3.116 | MP.3.123 |  | PE.3.136 |  | RM.3.147 | CA.3.227 |  | SC.3.180 | SI.2.216 |
| AC.2.007 |  | AU.3.048 |  | CM.3.067 | IA.2.082 | IR.3.099 | 4% | MP.3.124 |  | 4% |  | RM.4.149 | 5% |  | SC.3.181 | SI.2.217 |
| AC.2.008 |  | AU.3.049 |  | CM.3.068 | IA.3.083 | IR.4.100 |  | MP.3.125 |  |  |  | RM.4.150 |  |  | SC.3.182 | SI.3.218 |
| AC.2.009 |  | AU.3.050 |  | CM.3.069 | IA.3.084 | IR.4.101 |  | 5% |  |  |  | RM.4.151 |  |  | SC.3.183 | SI.3.219 |
| AC.2.010 |  | AU.3.051 |  | CM.4.073 | IA.3.085 | IR.5.106 |  |  |  |  |  | RM.4.148 |  |  | SC.3.184 | SI.3.220 |
| AC.2.011 |  | AU.3.052 |  | CM.5.074 | IA.3.086 | IR.5.102 |  |  |  |  |  | RM.5.152 |  |  | SC.3.185 | SI.4.221 |
| AC.2.013 |  | AU.4.053 |  | 7% | 7% | IR.5.108 |  |  |  |  |  | RM.5.155 |  |  | SC.3.186 | SI.5.222 |
| AC.2.015 |  | AU.4.054 |  |  |  | IR.5.110 |  |  |  |  |  | 7% |  |  | SC.3.187 | SI.5.223 |
| AC.2.016 |  | AU.5.055 |  |  |  | 8% |  |  |  |  |  |  |  |  | SC.3.188 | 8% |
| AC.3.017 |  | 8% |  |  |  |  |  |  |  |  |  |  |  |  | SC.3.189 |  |
| AC.3.018 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.3.190 |  |
| AC.3.019 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.3.191 |  |
| AC.3.012 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.3.192 |  |
| AC.3.020 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.3.193 |  |
| AC.3.014 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.4.197 |  |
| AC.3.021 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.4.228 |  |
| AC.3.022 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.4.199 |  |
| AC.4.023 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.4.202 |  |
| AC.4.025 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.4.229 |  |
| AC.4.032 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.5.198 |  |
| AC.5.024 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.5.230 |  |
| 15% |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.5.208 |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 16% |  |

**31% is Access Control (AC) and Systems & Communication Protection (SC)**

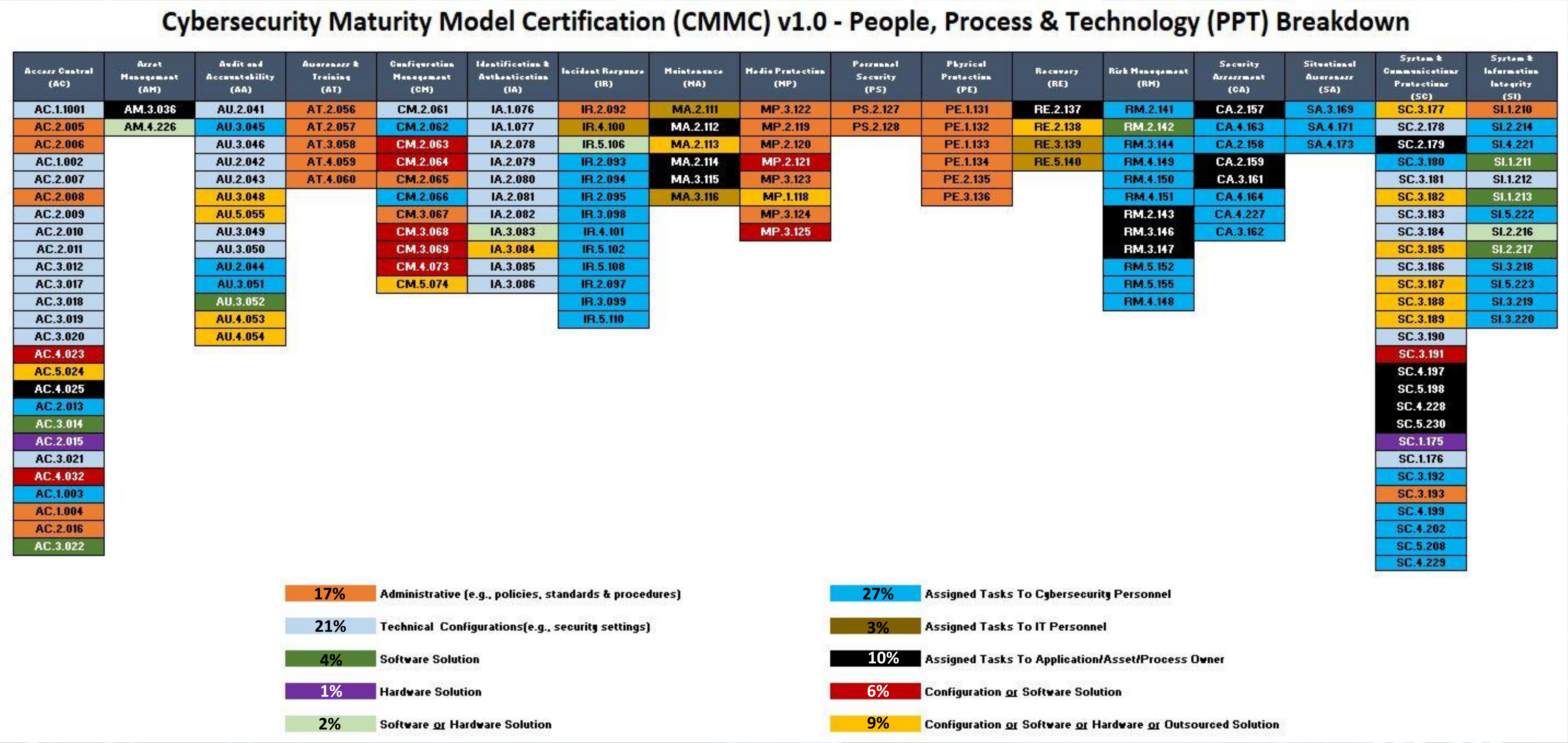
| CMMC Level 1 | CMMC Level 2 | CMMC Level 3 | CMMC Level 4 | CMMC Level 5 |
|---|---|---|---|---|

# CMMC Capabilities

| Domain | Capability |
|---|---|
| **Access Control (AC) – 15%** | - Establish system access requirements<br>- Control internal systems access<br>- Control remote systems access<br>- Limit data access to authorized users and processes |
| **Asset Management (AM) – 1%** | - Identify and document assets |
| **Audit & Accountability (AU) – 8%** | - Define audit requirements<br>- Perform auditing<br>- Identify and protect audit information<br>- Review and manage audit logs |
| **Awareness & Training (AT) – 3%** | - Conduct security awareness training<br>- Conduct training |
| **Configuration Management (CM) – 7%** | - Establish configuration baselines<br>- Perform configuration and change management |
| **Identification & Authentication (IA) – 7%** | - Grant access to authenticated identities |
| **Incident Response (IR) – 8%** | - Plan incident response<br>- Detect and report events<br>- Develop and implement a response to a declared incident<br>- Perform post incident reviews<br>- Test incident response |
| **Maintenance (MA) – 4%** | - Manage maintenance |

| Domain | Capability |
|---|---|
| **Media Protection (MP) – 5%** | - Identify and mark media<br>- Protect and control media<br>- Sanitize media<br>- Protect media during transport |
| **Personnel Security (PS) – 1%** | - Screen Personnel<br>- Protect CUI during personnel actions |
| **Physical Protection (PE) – 4%** | - Limit physical access |
| **Recovery (RE) – 2%** | - Manage backups |
| **Risk Management (RM) – 7%** | - Identify and evaluate risk<br>- Manage risk |
| **Security Assessment (CA) – 5%** | - Develop and manage a Systems Security Plan (SSP)<br>- Define and manage controls<br>- Perform code reviews |
| **Situational Awareness (SA) – 2%** | - Implement threat monitoring |
| **Systems & Communication Protection (SC) – 16%** | - Define security requirements for systems and communications<br>- Control communications at system boundaries |
| **System & Information Integrity (SI) – 8%** | - Identify and manage information flaws<br>- Identify malicious content<br>- Perform network and system monitoring<br>- Implement advanced email protections |

# CMMC – People, Process & Technology (PPT)



## Cybersecurity Maturity Model Certification (CMMC) v1.0 - People, Process & Technology (PPT) Breakdown

| Access Control (AC) | Asset Management (AM) | Audit and Accountability (AA) | Awareness & Training (AT) | Configuration Management (CM) | Identification & Authentication (IA) | Incident Response (IR) | Maintenance (MA) | Media Protection (MP) | Personnel Security (PS) | Physical Protection (PE) | Recovery (RE) | Risk Management (RM) | Security Assessment (CA) | Situational Awareness (SA) | System & Communications Protections (SC) | System & Information Integrity (SI) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AC.1.1001 | AM.3.036 | AU.2.041 | AT.2.056 | CM.2.061 | IA.1.076 | IR.2.092 | MA.2.111 | MP.3.122 | PS.2.127 | PE.1.131 | RE.2.137 | RM.2.141 | CA.2.157 | SA.3.169 | SC.3.177 | SI.1.210 |
| AC.2.005 | AM.4.226 | AU.3.045 | AT.2.057 | CM.2.062 | IA.1.077 | IR.4.100 | MA.2.112 | MP.2.119 | PS.2.128 | PE.1.132 | RE.2.138 | RM.2.142 | CA.4.163 | SA.4.171 | SC.2.178 | SI.2.214 |
| AC.2.006 |  | AU.3.046 | AT.3.058 | CM.2.063 | IA.2.078 | IR.5.106 | MA.2.113 | MP.2.120 |  | PE.1.133 | RE.3.139 | RM.3.144 | CA.2.158 | SA.4.173 | SC.2.179 | SI.4.221 |
| AC.1.002 |  | AU.2.042 | AT.4.059 | CM.2.064 | IA.2.079 | IR.2.093 | MA.2.114 | MP.2.121 |  | PE.1.134 | RE.5.140 | RM.4.149 | CA.2.159 |  | SC.3.180 | SI.1.211 |
| AC.2.007 |  | AU.2.043 | AT.4.060 | CM.2.065 | IA.2.080 | IR.2.094 | MA.3.115 | MP.3.123 |  | PE.2.135 |  | RM.4.150 | CA.3.161 |  | SC.3.181 | SI.1.212 |
| AC.2.008 |  | AU.3.048 |  | CM.2.066 | IA.2.081 | IR.2.095 | MA.3.116 | MP.1.118 |  | PE.3.136 |  | RM.4.151 | CA.4.164 |  | SC.3.182 | SI.1.213 |
| AC.2.009 |  | AU.5.055 |  | CM.3.067 | IA.2.082 | IR.3.098 |  | MP.3.124 |  |  |  | RM.2.143 | CA.4.227 |  | SC.3.183 | SI.5.222 |
| AC.2.010 |  | AU.3.049 |  | CM.3.068 | IA.3.083 | IR.4.101 |  | MP.3.125 |  |  |  | RM.3.146 | CA.3.162 |  | SC.3.184 | SI.2.216 |
| AC.2.011 |  | AU.3.050 |  | CM.3.069 | IA.3.084 | IR.5.102 |  |  |  |  |  | RM.3.147 |  |  | SC.3.185 | SI.2.217 |
| AC.3.012 |  | AU.2.044 |  | CM.4.073 | IA.3.085 | IR.5.108 |  |  |  |  |  | RM.5.152 |  |  | SC.3.186 | SI.3.218 |
| AC.3.017 |  | AU.3.051 |  | CM.5.074 | IA.3.086 | IR.2.097 |  |  |  |  |  | RM.5.155 |  |  | SC.3.187 | SI.5.223 |
| AC.3.018 |  | AU.3.052 |  |  |  | IR.3.099 |  |  |  |  |  | RM.4.148 |  |  | SC.3.188 | SI.3.219 |
| AC.3.019 |  | AU.4.053 |  |  |  | IR.5.110 |  |  |  |  |  |  |  |  | SC.3.189 | SI.3.220 |
| AC.3.020 |  | AU.4.054 |  |  |  |  |  |  |  |  |  |  |  |  | SC.3.190 |  |
| AC.4.023 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.3.191 |  |
| AC.5.024 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.4.197 |  |
| AC.4.025 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.5.198 |  |
| AC.2.013 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.4.228 |  |
| AC.3.014 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.5.230 |  |
| AC.2.015 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.1.175 |  |
| AC.3.021 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.1.176 |  |
| AC.4.032 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.3.192 |  |
| AC.1.003 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.3.193 |  |
| AC.1.004 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.4.199 |  |
| AC.2.016 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.4.202 |  |
| AC.3.022 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.5.208 |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | SC.4.229 |  |

| | | | |
|---|---|---|---|
| 17% | Administrative (e.g., policies, standards & procedures) | 27% | Assigned Tasks To Cybersecurity Personnel |
| 21% | Technical Configurations(e.g., security settings) | 3% | Assigned Tasks To IT Personnel |
| 4% | Software Solution | 10% | Assigned Tasks To Application/Asset/Process Owner |
| 1% | Hardware Solution | 6% | Configuration or Software Solution |
| 2% | Software or Hardware Solution | 9% | Configuration or Software or Hardware or Outsourced Solution |

https://www.complianceforge.com/

# CMMC Accreditation Body (AB)

- Late Fall, the CMMC Accreditation Body (AB) was created. It is made up of unbiased parties that will oversee the training, quality and administration of the CMMC third-party assessment organizations (C-3PAOs).
- The AB will be responsible for training and certifying candidate C-3PAOs and individual assessors.
- Their goal is to train, test, and license up to 10,000 CMMC assessors.

# Certified Third-Party Assessment Organizations (C3PAO)

- A C3PAO is an organization where licensed assessors will come together hone their skills and register their licenses.
- Each C3PAO will need to be certified by the CMMC-AB prior to deploying its assessors into the field.
- Unknown:
  - When you will be able to register to become an official C3PAO.  Think Q2 2020
  - The rules for what it takes to be a C3PAO in good standing.
  - The fees or details associated with the process. The CMMC-AB is a nonprofit. Fees will reflect the costs of "providing an independent, national organization with a leading-edge customer experience."

# Assessors

- Assessors will receive a license from the CMMC-AB after completing the required training and passing an examination.
- Assessors will NOT work for the CMMC-AB but will work for a C3PAO.
- Assessors will receive a license at a level that matches the assessments they are permitted to conduct.
- Experience requirements for higher-level assessors are likely to be required but are not yet determined.
- Assessors are required to obtain a security clearance.  The specific clearance levels are not yet determined.
- Unknown:
    - Availability dates for training are not yet known.  Expect late Q1 or Q2 2020.
    - Training , content, structure, levels etc.  are not yet determined.
    - Fees, locations, or authorized organizations providing training.

# CMMC Timeline

- Selecting and training third-party vendors (C-3PAO) (Late Spring)
- New Defense Federal Acquisition Regulation (DFAR) (Early Summer)
- They plan to target 10 RFIs and RFPs.
    - For each of those, there are an estimated 150 subcontractors involved.
    - Contracts would represent a mix of mostly levels 1 and 3 with “maybe one or two that have the 4 or 5” level.
- DoD expects CMMC to take five years to fully roll out, and not really get going until 2021. DoD expects the third-party assessors to certify about 1,500 vendors in 2021, 7,500 more in 2022 and 25,000 more by 2023.
- By fiscal year 2026, all new Defense Department contracts will contain CMMC requirements that companies must meet to win the award.

# Facts Today

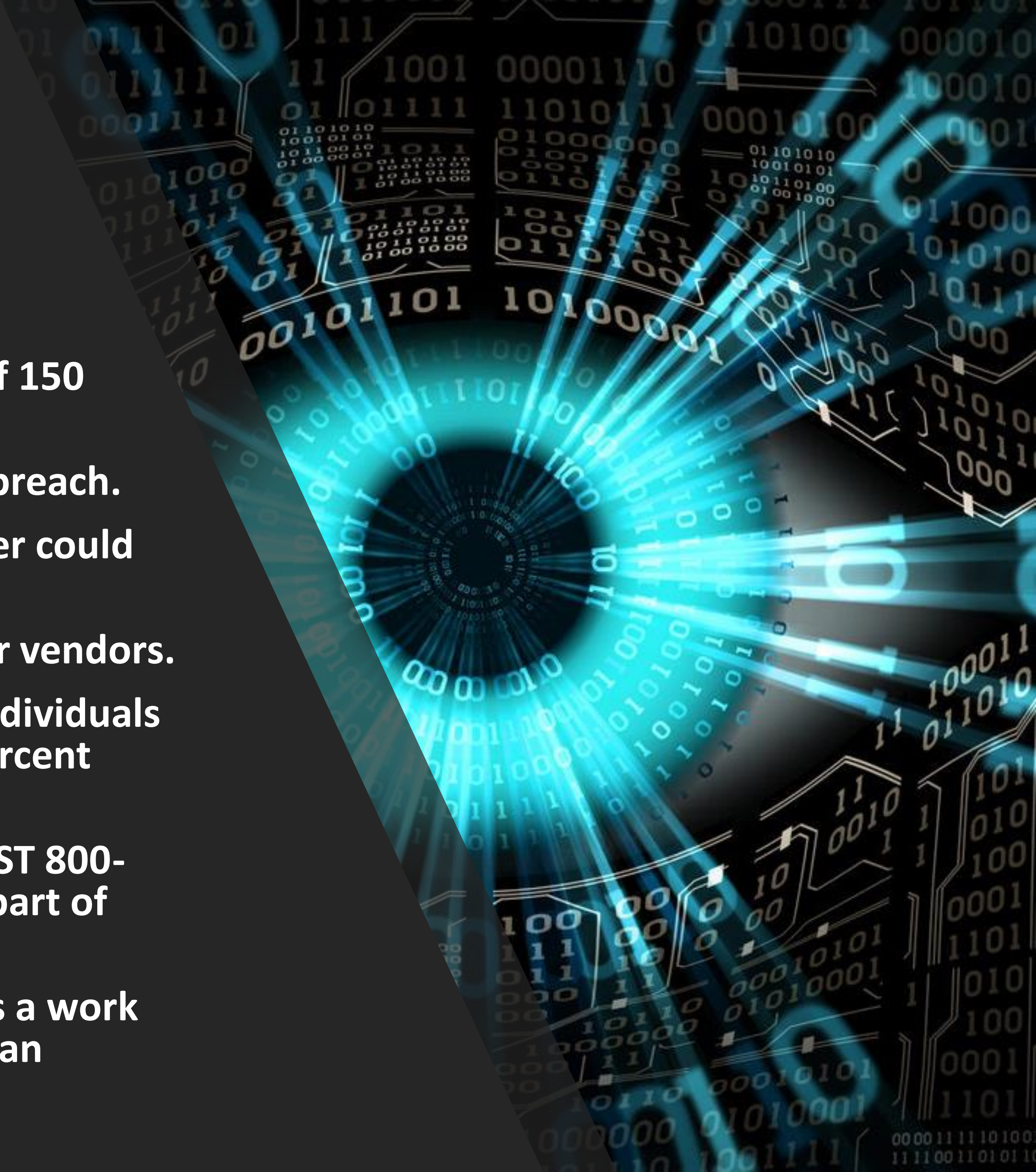
- The CMMC Standard is not yet finalized and no Assessors or C3PAOs are formally accredited or certified by the CMMC-AB.
- The CMMC-AB will publish a publicly available list of Assessors after the standard is complete, the training is developed, and Assessors are certified to provide CMMC certification.
- The CMMC-AB is building the C3PAO accreditation process with formal adoption and approval by the CMMC AB in the coming months.
- Certification requirement WILL NOT apply to current contracts.
- When implemented, all companies conducting business with the DoD must be certified.
- There are no fines for not complying – just loss of contract(s)
- The certifications are expected to be valid for three years before they must be renewed.
- Still need to meet requirements of DFARS 7012 (NIST 800-171, SSP, POA&M)

# Impacts

- **Future work with DoD will require a CMMC level of certification**
- **Undetermined financial cost to obtain each level**
- **Cost of Third Part Assessors**
- **Cost of preparing for assessment**
- **Current contracts not affected, but recompete will have new requirement.**
- **Prime Contractors impacts**
- **Subcontractor impacts**

# CMMC Is Still Unknown in Defense Industrial Base (DIB)

- Tier 1 Cyber in November conducted a survey of 150 government contractors.
- 27% admitted they are unprepared for a cyber breach.
- 58% were unfamiliar with CMMC - only a quarter could correctly identify the acronym.
- 12% were confident in the cybersecurity of their vendors.
- 40% said they only have between one and 10 individuals dedicated to information technology, and 10 percent didn’t have a dedicated IT professional at all.
- 44% said they were still working to meet the NIST 800-171 requirements — which are expected to be part of level 3 CMMC standards.
- 41% said their cyber incident response plan was a work in progress, and only 20 percent said they have an incident response plan in place.



# Don’ts

- **Don’t post your CMMC level certification on your website – telling the world your vulnerabilities**
- **Don’t contract outside assistance saying they “can certify you” in CMMC –**
  - **They may “assist” but be careful of Conflict of Interest.**
  - **The accreditation body, which is independent of DoD, is considering sending “cease and desist” letters to any company saying they can get another vendor certified under CMMC.**
- **Don’t take it lightly – if you are not at the level required, you will not be awarded the contract.**
- **Don’t hesitate to start preparing – waiting for an RFP and being ready at time of award is dangerous**
- **Don’t rely on the one IT person to guide you – has to be a group effort and leadership fully involved**

# Targeted Audience on Self-Assessment

**This serves Information Security, and Privacy Professionals Including Individuals with:**

- **System Development Responsibilities** (*e.g., Program Managers, System Developers, System Owners, Systems Integrators, System Security Engineers*);
- **Information Security Assessment and Monitoring Responsibilities (***e.g., System Evaluators, Assessors, Independent Verifiers/Validators, Auditors, Analysts, System Owners*);
- **Information Security, Privacy, Risk Management, Governance, and Oversight Responsibilities** (*e.g., Authorizing Officials, Chief Information Officers, Chief Privacy Officers, Chief Information Security Officers, System Managers, Information Security Managers*);
- **Information Security Implementation and Operational Responsibilities** (*e.g., System Owners, Information Owners/Stewards, Mission and Business Owners, Systems Administrators, System Security Officers*).

# Do's

- **Be proactive and assess where you stand (Example: Do you have FCI or CUI in your network?)**
- **Who are the prime contractors you work with, and what are they doing/saying about CMMC?**
- **Assess the CMMC level of your current contracts**
- **Based on assessment, determine costs and budget**
- **If you haven't, start practicing good cyber hygiene**
- **Ensure your team is prepared for any cyber incident**
- **Train, train, and train your personnel on cybersecurity risks (i.e., phishing)**
- **Review current policies and procedures**
- **Review/update your teaming agreements, subcontracts, NDAs and other contracts with 3rd parties**

**Minimum Be Level 1**

# Resources

- CMMC

| | |
|---|---|
| Home Page: | https://www.acq.osd.mil/cmmc/draft.html |
| CMMC Accreditation Board: | https://www.cmmcab.org/ |
| CMMC Assessors: | https://www.cmmcab.org/assessors |
| C3PAOs: | https://www.cmmcab.org/c3pao |
| Training: | https://www.cmmcab.org/trainers |

- CUI
  - DODINST 5200.48 (CUI)
    https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF

# Questions?

# Back-Ups

| Control | CMMC Clarification | Reference |
|---|---|---|
| **AC.1.001**<br>**Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).** | **Control who can use company computers and who can log on to the company network. Limit the services and devices, like printers, that can be accessed by company computers. Set up your system so that unauthorized users and devices cannot get on the company network.**<br>**Example:**<br>You oversee IT for your company. You give a username and password to every employee who uses a company computer for their job. No one can use a company computer without a username and a password. You give a username and password to those employees you know have permission to be on the systems. When an employee leaves the company, you disable their username and password immediately.<br>A coworker from the marketing department tells you their boss wants to buy a new multi-function printer/scanner/fax device and make it available on the company network. You explain that the company controls system and device access to the network and will stop non-company systems and devices unless they already have permission to access the network. You work with the marketing department to grant permission to the new printer/scanner/fax device to connect to the network, then install it. | • **FAR Clause 52.204-21**<br>• **NIST SP 800-171**<br>• **CIS Controls v.7.1**<br>• **NIST CSF v.1.1**<br>• **CERT RMM v.1.2**<br>• **NIST 800-53 Rev4**<br>• **AU ASCC Essential Flight** |
| **AC.1.002**<br>**Limit information system access to the types of transactions and functions that authorized users are permitted to execute.** | **Make sure to limit user/employees to only the information systems, roles, or applications they are permitted to use and that are needed for their jobs.**<br>**Example:**<br>You oversee payroll for the company and need access to certain company financial information systems. You work with IT to set up the systems so that when users log onto the company's network, only those employees you allow can use payroll applications and access payroll data. Because of this good access control, your coworkers in the Shipping Department cannot access information about payroll or paychecks. | • **FAR Clause 52.204-21**<br>• **NIST SP 800-171**<br>• **CIS Controls v.7.1**<br>• **NIST CSF v.1.1**<br>• **CERT RMM v.1.2**<br>• **NIST 800-53 Rev4** |
| **AC.1.003**<br>**Verify and control/limit connections to and use of external information.** | **Make sure to control and manage connection between your company network and outside networks, such as the public internet or a network that does not belong to your company. Be aware of applications that can run by outside systems. Control and limit personal devices like laptops, tablets, and phones accessing the company networks and information. You can also choose to limit how and when your network is connected to outside systems and/or decide that only certain employees can connect to outside systems from network services.**<br>**Example:**<br>You help manage IT for your employer. You and your coworkers are working on a big proposal, and all of you will put in extra hours over the weekend to get it done. Part of the proposal includes Federal Contract Information (FCI). FCI is information that you and your company can get from doing work for the Federal government. Because FCI is not shared publicly, you remind your coworkers to use their company laptops, not personal laptops or tablets, when working on the proposal over the weekend. | • **FAR Clause 52.204-21**<br>• **NIST SP 800-171**<br>• **CIS Controls v.7.1**<br>• **NIST CSF v.1.1**<br>• **CERT RMM v.1.2**<br>• **NIST 800-53 Rev 4** |
| **AC.1.004**<br>**Control information posted or processed on publicly accessible information systems.** | **Do not allow sensitive information, including Federal Contract Information (FCI), which may include CUI, to become public. It is important to know which users/employers can publish information on publicly accessible systems, like your company website. Limit and control information that is posted on your company's website(s) that can be accessed by the public.**<br>**Example:**<br>You are head of marketing for your company and want to become better known by your customers. So, you decide to start issuing press releases about your company projects. Your company gets FCI from doing work for the Federal government. FIC is information that should not be publicly shared. Because you recognize the need to control sensitive information, including FCI, you carefully review all information before posting it on the company website or releasing to the public. You allow only certain employees to post to the website. | **Return** |