ACQUISITION
AND SUSTAINMENT

OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

CYBERSECURITY MATURITY MODEL CERTIFICATION

EXECUTIVE STEERING GROUP AND WORKING GROUP FOR IMPLEMENTATION

STRATEGIC VISION

- Safeguard sensitive information to enable and protect the warfighter
- Dynamically enhance DIB cybersecurity to meet evolving threats
- Ensure accountability while minimizing barriers to compliance with DoD requirements
- Contribute towards instilling a collaborative culture of cybersecurity and cyber resilience
- Maintain public trust through high professional and ethical standards

OBJECTIVES

CMMC Executive Steering Group

- Provides strategic level guidance to the Working Group (WG)
- Reviews courses of action (COAs)
- Approves implementation plan
- Syndicates decisions with USD(A&S) and other senior leaders in the Department and USG

CMMC Working Group

- Develops executable COAs and a viable implementation plan in accordance with guidance from the Executive Steering Group (ESG)
- Recommends potential programmatic changes to CMMC
- Provides a rulemaking strategy
- Assesses budget and resources required to support CMMC PMO
- Develops a public affairs plan, to include Congress, industry members, and media
- Syndicates proposals with external stakeholders in the Department and USG

MILESTONES

- By June 4, 2021: Stand up CMMC ESG and WG
- By June 11: Develop detailed weekly plan and key milestones for 120-day effort
- By June 18: Approve public engagement plan
- By June 25: Deliver update to CMMC-AB on near-term direction for CMMC implementation
- … (additional milestones to be defined by the WG)
- By November 1, 2021: CMMC WG present an implementation plan to the CMMC ESG for review and approval
- Throughout review: CMMC WG conduct bi-weekly progress checks with the CMMC ESG

ROLES AND RESPONSIBILITIES

- Co-Chairs of the CMMC ESG will
  - Identify and prioritize high-level issues to be addressed by the ESG and in turn the WG
  - Report progress and solicit feedback from USD(A&S)
  - Coordinate WG priorities and progress with other senior leaders in the Department, other agencies, and Congress, as required
- ESG members will
  - Participate in ESG meeting on bi-weekly basis, or as agreed upon with ESG co-chairs
  - Advise on CMMC impacts from their respective organizations' viewpoints
  - Contribute time and SME resources to support the CMMC WG priorities
- Executive Secretary and WG Chair will
  - Create and maintain a 120-day work plan aligned to co-chairs' priorities
  - Develop a detailed agenda for each ESG meeting, including matters for discussion, COAs, analysis, recommendations, and due-outs
  - Incorporate findings and inputs into consolidated read-aheads for ESG members
  - Coordinate and facilitate ESG and WG meetings
- WG members will
  - Meet weekly or at the discretion of the WG chair
  - Contribute to the 120-day work plan, including bi-weekly decision points and other milestones
  - Drive analysis and develop recommendations for ESG consideration; solicit SME input from respective offices and teams as necessary
  - Solicit and consider input from additional key stakeholders, including defense agencies, services, and joint staff

EXECUTIVE STEERING GROUP MEMBERS

Co-chairs

- Jesse Salazar, DASD for Industrial Policy, OUSD(A&S)
- Mieke Eoyang, DASD for Cyber Policy, OUSD(P)
- David Frederick, Executive Director (CYBERCOMM)
- David McKeown, Deputy CIO

ESG members

- Stacy Bostjanick, CISO(A&S)
- Doug Bush, ASA(ALT)
- RDML William Chase, Deputy Principal Cyber Advisor
- Darlene Costello, SAF/AQ – *pending confirmation*
- Mike Glennon, OGC
- Mitch Komaroff, DoD CIO
- (b)(6), OUSD(A&S)/IndPol
- (b)(6), OSD(PA)
- (b)(6), OUSD(A&S)/DPC
- (b)(6), OUSD(I&S)
- (b)(6), ASN(RD&A) – *pending confirmation*
- (b)(6), *OUSD(R&E) –pending confirmation*

Executive Secretary and Working Group Chair: (b)(6), Director, CMMC, CISO(A&S)

WORKING GROUP MEMBERS

WG Permanent members

- (b)(6), CISO(A&S)
- (b)(6), OUSD(A&S)
- (b)(6), DoD CIO
- (b)(6), DCMA
- (b)(6), OSD(PA)
- (b)(6), CISO(A&S)
- (b)(6), OUSD(I&S)
- (b)(6), OUSD(P)
- (b)(6), OUSD(R&D)
- (b)(6), OGC
- (b)(6), NSA

WG Rotating members and SMEs (involved as needed)

- (b)(6), WHS
- (b)(6), OUSD(A&S)/DPC
- (b)(6), OUSD(P)
- (b)(6), DC3
- (b)(6), DIA
- Services acquisition action officers, as designated by the Service Acquisition Executives
- Others as designated by the ESG Co-Chairs and WG Chair

OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION
AND SUSTAINMENT

READ-AHEAD FOR THE PTDO USD(A&S)
CMMC Revised Implementation In Progress Review
Date/Time: 16 Sep 21, 1:00 PM
3A912A

From: Jesse Salazar, DASD, IndPol, 703-697-0051

Lead: Buddy Dees/OUSD(A&S)/CMMC PMO

Key Attendees:

Mr. John Sherman, Acting DoD CIO
Dr. Kelly Fletcher, Principal Deputy CIO
Jesse Salazar, DASD, IndPol / CMMC Executive Steering Group (ESG) Co-Chair
Mr. Dave McKeown, DCIO Cybersecurity / CMMC ESG Co-Chair
Mr. Dave Frederick, Executive Director, USCYBERCOM / CMMC ESG Co-Chair
Ms. Mieke Eoyang, DASD Cyber Policy / ESG Co-Chair
(b)(6), OUSD(A&S)/IndPol

Objective:

- Provide the PTDO USD(A&S) and Acting DoD CIO with an In-Progress Review (IPR) of the CMMC ESG's progress in the analysis of recommendations from an independent review of the CMMC program's implementation. (TAB A)

Background:

- The DSD directed an internal review of the CMMC program's implementation, to include the approach to the CMMC accreditation process, and the identification of potential barriers for industry to achieving CMMC certification
- The PTDO USD(A&S) established a Tiger Team on 18 Mar 2021 to conduct the review and the Tiger Team out briefed 8 recommendations to the DSD on 13 May 2021.
- The DSD directed further analysis into the feasibility of implementing the recommendations and to develop a revised CMMC Implementation Plan within 150-days.
- A senior-level cross functional ESG was created to provide guidance to a CMMC Working Group that conducted the additional analysis.
- The ESG is planning to outbrief the DSD in the early Nov 2021 timeframe.

Attachments:

1. TAB A (In Progress Review Briefing)

Coordination:

- None.

Prepared by: (b)(6), ODASD/IndPol, (b)(6) (USAXXXXX-21)

OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION
AND SUSTAINMENT

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP (SEE DISTRIBUTION)
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Cybersecurity Maturity Model Certification Revised Implementation

The Defense Industrial Base (DIB) is the target of continuous cyber-attacks and the exfiltration of Controlled Unclassified Information, other sensitive information, and intellectual property has put the warfighter and our nation at risk. In response, the Department of Defense (DoD) is undertaking several efforts to protect the data and enhance the cybersecurity of defense contractors' unclassified networks while also striking a balance with affordability and competition. Among these efforts is the Cybersecurity Maturity Model Certification (CMMC) program.

The Department issued an interim rule on September 29, 2020 to amend the Defense Federal Acquisition Regulation Supplement to implement the CMMC framework in order to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain. This interim rule, which became effective on November 30, 2020, includes a five year phased rollout to minimize financial impacts to the industrial base, especially small entities, and disruption to the supply chain.

In an effort to continue to improve the CMMC program, I directed an independent team to conduct a 30-day review and evaluation focused on the implementation of CMMC. More specifically, I tasked this team to assess and provide recommendations on (i) the Department's approach to the CMMC concept of operations, governance structure, accreditation process, and standards of conduct within the ecosystem, as well as (ii) mitigating potential barriers for industry to achieve CMMC certifications. With my concurrence, the team briefed the Deputy Secretary of Defense on its findings and recommendations.

Based on the outcome of this outbrief, I established an executive steering group and an associated working group to develop a revised CMMC implementation plan over the next 120 days. At the conclusion of this 120-day effort and my approval, the executive steering group will provide the updated implementation plan to the Deputy Secretary of Defense.

The Department remains committed to working with our DIB partners to mitigate cybersecurity threats that target our supply chain and seek to undercut our technological advantages. If you have any questions regarding this matter, please contact my point of contact, Ms. Stacy Bostjanick, at stacy.bostjanick.civ@mail.mil or (202) 819-2158.

Stacy A. Cummings
Principal Deputy Assistant Secretary of Defense
(Acquisition)
Performing the Duties of Under Secretary of
Defense for Acquisition and Sustainment

DISTRIBUTION:
Chief Management Officer of the Department of Defense
Secretaries of the Military Departments
Chairman of the Joint Chiefs of Staff
Under Secretaries of Defense
Chief of the National Guard Bureau
General Counsel of the Department of Defense
Director of Cost Assessment and Program Evaluation
Inspector General of the Department of Defense
Director of Operational Test and Evaluation
Chief Information Officer of the Department of Defense
Assistant Secretary of Defense for Legislative Affairs
Assistant to the Secretary of Defense for Public Affairs
Director of Net Assessment

Cybersecurity Maturity Model Certification

Version 2.0

November 17, 2021

Note: The information in this presentation reflects the Department's strategic intent with respect to the CMMC program. The Department will be engaging in rulemaking and internal resourcing as part of implementation, and program details are subject to change during these processes.

CMMC 2.0 Model

CMMC 2.0 model is streamlined to three versus five levels

- **Eliminates CMMC 1.0 Levels 2 and 4:** Developed as transition levels and never intended to be assessed requirements
- **Establishes three progressively sophisticated levels, depending on the type of information:**
  - Level 1 (Foundational) – for companies with FCI only; information requires protection but is not critical to national security
  - Level 2 (Advanced) – for companies with CUI
  - Level 3 (Expert) – for the highest priority programs with CUI

Requirements will mirror NIST SP 800-171 and NIST SP 800-172

- **Eliminates all CMMC unique practices and maturity processes:** Work with NIST to address identified gaps in the NIST SP 800-171
- **Aligns Level 2 with NIST SP 800-171**
- **Level 3 will use a subset of NIST SP 800-172 requirements**

Simplifies the CMMC standard for companies, while safeguarding critical Department information

CMMC 2.0 Assessments

CMMC Level 1 (Foundational) will require DIB company self-assessments

CMMC Level 2 (Advanced) may require third-party or self-assessments, depending on the type of information

- **Requires third-party assessments for prioritized acquisitions:** Companies will be responsible for obtaining an assessment and certification prior to contract award
- **Requires self-assessments for other non-prioritized acquisitions:** Companies will complete and report a CMMC Level 2 self-assessment and submit senior official affirmations to SPRS

CMMC Level 3 (Expert) will be assessed by government officials

Eases assessment requirements for companies not handling information related to prioritized acquisitions

Allowance of POA&Ms and Waivers

CMMC 2.0 will allow limited use of POA&Ms

- **Strictly time-bound:** Potentially 180 days; Contracting Officers can use normal contractual remedies to address a DIB contractor's failure to meet their cybersecurity requirements after the defined timeline
- **Limited use:** Will not allow POA&Ms for highest-weighted requirements; will establish a "minimum score" requirement to support certification with POA&Ms

Waivers will be allowed on a very limited basis, accompanied by strategies to mitigate CUI risk

- **Only allowed in select mission critical instances:** Government program office will submit the waiver request package including justification and risk mitigation strategies
- **Strictly time bound:** Timing to be determined on a case-by-case basis; Contracting Officers can use normal contractual remedies to address a DIB contractor's failure to meet their cybersecurity requirements after the defined timeline
- **Will require senior DoD approval** to minimize potential misuse of the waiver process

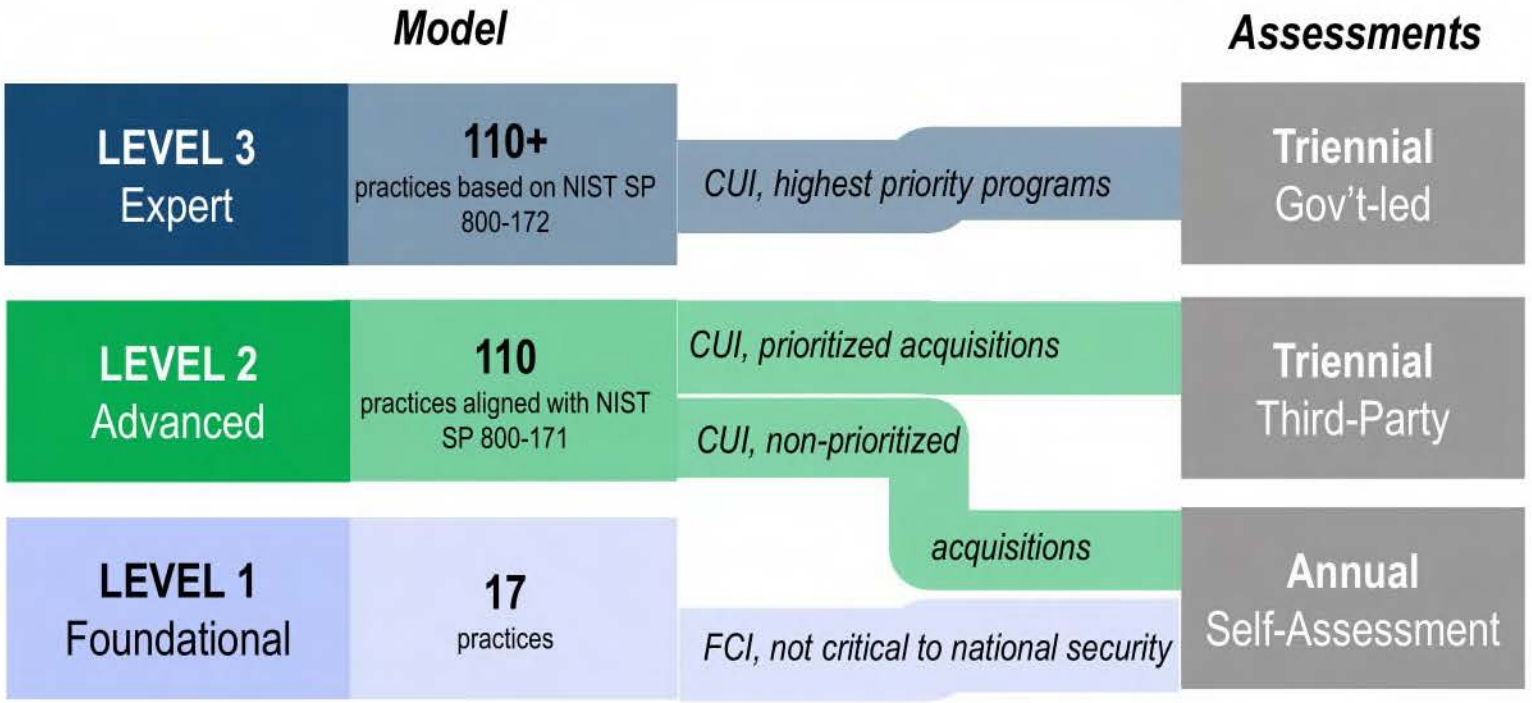
Limited use of POA&Ms and waivers could allow the Department and DIB companies flexibility to meet evolving threats and make risk-based decisions

Rulemaking – Codifying CMMC 2.0

Changes will be released through a interim rule. A 60-day public comment period and concurrent congressional review will be included prior to the rule becoming effective

- DoD has **mandatory rulemaking obligations** for CMMC that must be addressed as part of the CMMC 2.0 implementation
  - Rulemaking under 32 CFR is required to establish the CMMC program
  - Rulemaking under 48 CFR is required to update the contractual requirements in the DFARS to implement the CMMC 2.0 program
  - The DoD is suspending the CMMC Piloting effort and mandatory CMMC certification
- Timeline to complete all rulemaking requirements will be 9 to 24 months; includes a mandatory 60-day public comment period and concurrent congressional review
  - The DoD will continue to encourage the DIB sector to enhance their cybersecurity posture during the interim period
  - The Department is exploring opportunities to provide incentives for contractors who voluntarily obtain a CMMC 2.0 Level 2 certification in the interim period
  - Until rulemaking formally implements CMMC 2.0, the DIB's participation in CMMC will be voluntary

CMMC 2.0 tailors model and assessment requirements to the type of information being handled



Note: The information in this presentation reflects the Department's strategic intent with respect to the CMMC program. The Department will be engaging in rulemaking and internal resourcing as part of implementation, and program details are subject to change during these processes.

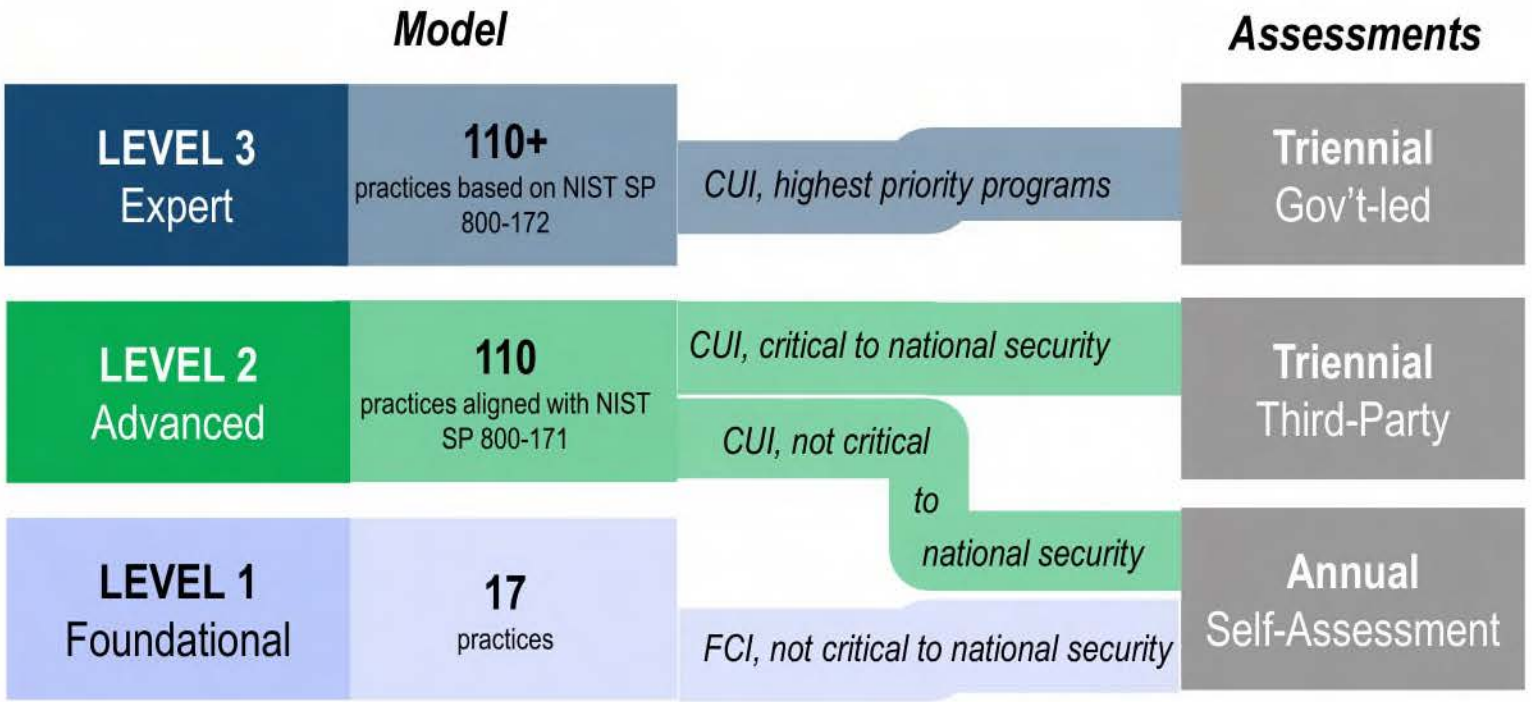
Questions?

Cybersecurity Maturity Model Certification Executive Steering Group

Industry Roundtable on CMMC 2.0

November 5, 2021

CMMC 2.0 tailors model and assessment requirements to the type of information being handled



Note: The information in this presentation reflects the Department's strategic intent with respect to the CMMC program. The Department will be engaging in rulemaking and internal resourcing as part of implementation, and program details are subject to change during these processes.

CMMC 2.0 Model

CMMC 2.0 model is streamlined to three versus five levels

- **Eliminates CMMC 1.0 Levels 2 and 4:** Developed as transition levels and never intended to be assessed requirements
- **Establishes three progressively sophisticated levels, depending on the type of information:**
  - Level 1 (Foundational) – for companies with FCI only; information requires protection but is not critical to national security
  - Level 2 (Advanced) – for companies with CUI
  - Level 3 (Expert) – for the highest priority programs with CUI

Requirements will mirror NIST SP 800-171 and NIST SP 800-172

- **Eliminates all CMMC unique practices and maturity processes:** Work with NIST to address identified gaps in the NIST SP 800-171
- **Aligns Level 2 with NIST SP 800-171**
- **Level 3 will use a subset of NIST SP 800-172 requirements**

Simplifies the CMMC standard for companies, while safeguarding critical Department information

CMMC 2.0 Assessments

CMMC Level 1 (Foundational) will require DIB company self-assessments

CMMC Level 2 (Advanced) may require third-party or self-assessments, depending on the type of information

- **Requires third-party assessments for acquisitions that involve information critical to national security:** Companies will be responsible for obtaining an assessment and certification prior to contract award
- **Requires self-assessments for other acquisitions:** Companies that are handling CUI deemed not critical to national security will complete and report a CMMC Level 2 self-assessment and submit senior official affirmations to SPRS

CMMC Level 3 (Expert) will be assessed by government officials

Eases assessment requirements for companies that do not handle information critical to national security

Allowance of POA&Ms and Waivers

CMMC 2.0 will allow limited use of POA&Ms

- **Strictly time-bound:** Potentially 180 days; Contracting Officers can use normal contractual remedies to address a DIB contractor's failure to meet their cybersecurity requirements after the defined timeline
- **Limited use:** Will not allow POA&Ms for highest-weighted requirements; will establish a "minimum score" requirement to support certification with POA&Ms

Waivers will be allowed on a very limited basis, accompanied by strategies to mitigate CUI risk

- **Only allowed in select mission critical instances:** Government program office will submit the waiver request package including justification and risk mitigation strategies
- **Strictly time bound:** Timing to be determined on a case-by-case basis; Contracting Officers can use normal contractual remedies to address a DIB contractor's failure to meet their cybersecurity requirements after the defined timeline
- **Will require senior DoD approval** to minimize potential misuse of the waiver process

Limited use of POA&Ms and waivers could allow the Department and DIB companies flexibility to meet evolving threats and make risk-based decisions

Rulemaking – Codifying CMMC 2.0

Changes will be released through a interim rule. A 60-day public comment period and concurrent congressional review will be included prior to the rule becoming effective

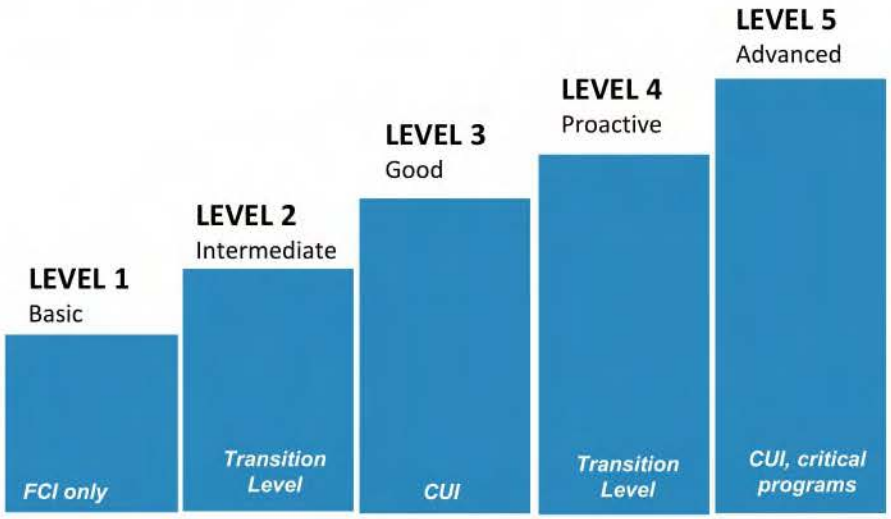
- DoD has **mandatory rulemaking obligations** for CMMC that must be addressed as part of the CMMC 2.0 implementation
  - Rulemaking under 32 CFR is required to establish the CMMC program
  - Rulemaking under 48 CFR is required to update the contractual requirements in the DFARS to implement the CMMC 2.0 program
  - The DoD is suspending the CMMC Piloting effort and mandatory CMMC certification
- Timeline to complete all rulemaking requirements will be 9 to 24 months; includes a mandatory 60-day public comment period and concurrent congressional review
  - The DoD will continue to encourage the DIB sector to enhance their cybersecurity posture during the interim period
  - The Department is exploring opportunities to provide incentives for contractors who voluntarily obtain a CMMC 2.0 Level 2 certification in the interim period
  - Until rulemaking formally implements CMMC 2.0, the DIB's participation in CMMC will be voluntary

Questions?

Back up

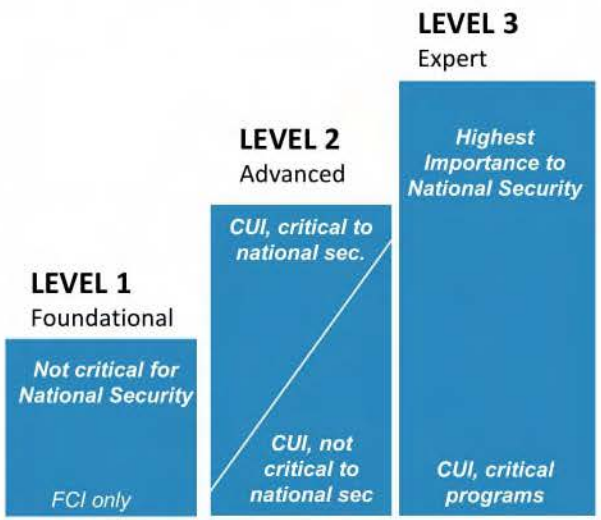
In sum, the revised CMMC framework is streamlined, operationally feasible, and protects critical information

CURRENT FRAMEWORK: CMMC 1.0



Model	17 practices	72 practices 2 maturity processes	130 practices 3 processes	156 practices 4 processes	171 practices 5 processes
Assessment	Third-party	None	Third-party	None	Third-party
Other					

REVISED FRAMEWORK: CMMC 2.0



	17 practices	110 practices	110+ practices
	Self-Assessment	• Third Party Assessments for critical national security information; • Self-Assessment for select programs	Govt-led Assessments
		POA&Ms and Waivers	POA&Ms and Waivers

DEFENSE ACQUISITION UNIVERSITY

Business, Cost Estimating and Financial Management Department

February 2011

TEACHING NOTE

ANALYSIS OF ALTERNATIVES

Patrick K. Morrow

INTRODUCTION

The ***Analysis of Alternatives (AoA)*** is a documented evaluation of the performance, operational effectiveness, operational suitability, and estimated costs of alternative systems to meet a capability need that has been identified through the Joint Capabilities Integration and Development Systems (JCIDS) process. The AoA assesses the advantages and disadvantages of various materiel alternatives being considered to satisfy the capability need. The AoA also considers the sensitivity of each alternative to possible changes to key assumptions or variables. The AoA is a key input to the process of defining the system capabilities set forth and further refined in the Capability Development Document (CDD).

Note: Where applicable, this teaching note has incorporated provisions of the Weapon Systems Acquisition Reform Act of 2009 (WSARA). As of the date this teaching note, the Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD (AT&L)) had not yet formally revised DoDI 5000.02 to reflect the requirements of that public law; however, that office had issued a Directive-Type Memorandum (DTM – 09-027) to institutionalize selected requirements of that law.

OVERVIEW:

Determination of DoD's need for a new capability, as well as the refinement of that capability, is accomplished through the JCIDS process, which is under the purview of the Office of the Joint Chiefs of Staff (OJCS). The JCIDS process is initiated through the execution of a Capabilities Based Assessment (CBA). The objective of the CBA is to validate capability gaps by providing the following: identification of the mission; the capabilities required and their associated operational characteristics and attributes; capability gaps and associated operational risks; an assessment of the viability of non-materiel solutions; and a potential recommendation on a type of solution to be pursued. If a non-materiel solution is recommended, or can be implemented independent of proposed materiel needs, a joint doctrine, organization, training, materiel, leadership and education, personnel, or facilities (DOTMLPF) Change Recommendation (DCR) is produced. However, if a materiel solution is required, an Initial Capabilities Document (ICD) is produced. When the ICD is approved as having the potential to satisfy the capability need with a materiel solution (i.e., hardware and/or software system acquisition), the Milestone Decision Authority (MDA) directs initiation of an AoA.

The AoA Study Plan, in conjunction with the ICD, helps to guide the Materiel Solution Analysis (MSA) phase of the acquisition life cycle. For potential and designated Acquisition Category (ACAT) I and IA programs, the AoA Study Guidance is approved by the Director, Cost

Assessment and Program Evaluation (D, CAPE). Following the Materiel Development Decision, the organization responsible for conducting the AoA develops the AoA Study Plan, coordinates it with the MDA, and submits it to the D, CAPE for approval prior to the start of the AoA. A study plan will typically contain the following sections, although it can (and should) be tailored or streamlined to support the given situation:

- Introduction
- Ground Rules
- Range of Alternatives
- Effectiveness Measures
- Effectiveness Analysis
- Cost Analysis
- Cost-Effectiveness Comparisons
- Organization and Management

The AoA shall assess the critical technology elements associated with the various concepts, including technology maturity, technical risks, and, if necessary, technology maturation and demonstration needs. If an existing system (i.e., the *status quo*) is a feasible alternative for obtaining the desired capability, this should also be evaluated in the AoA. The MSA phase ends when the MDA approves the materiel solution resulting from the AoA and approves the associated Technology Development Strategy (TDS). Later in the acquisition process, the initial AoA may be updated or superseded, as warranted, by then-existing circumstances.

Ideally, a system's operational effectiveness enables it to meet or exceed capability needs identified by the JCIDS process. Operational effectiveness is achieved if the system satisfies operational requirements (thresholds and objectives) specified in the Capability Development Document (CDD), which builds upon the ICD by detailing the operational performance parameters necessary to design the proposed system. As stated in CJCSI 3170.01 (the Joint Chiefs of Staff instruction that describes the JCIDS process), a capability is "the ability to achieve a desired effect under specified standards and conditions through combinations of means and ways … to perform a set of tasks to execute a specified course of action." The description of a capability should be "general enough so as to not prejudice decisions in favor of a particular means of implementation, but specific enough to evaluate alternative approaches to implement the capability. Achieving a stated capability is possible only if the system meets specified design, performance and Measures of Effectiveness (MOE) thresholds. For example, a vehicle's operational effectiveness might be described by its weight, accuracy, speed, range, horsepower, survivability, etc.

Design, performance, and MOE parameters commonly serve as the basis of a system's life cycle cost estimate. For example, a designer must specify vehicle engine horsepower and fuel consumption rate to enable a cost analyst to estimate vehicle engine life cycle cost. A less traditional AoA scenario exists when cost is fixed (i.e., cost as an independent variable (CAIV)). In a CAIV scenario, the AoA design and performance trade space are constrained by a pre-determined cost threshold. For example, the program manager (PM) specifies a vehicle engine life cycle cost threshold and objective *prior* to the designer proposing horsepower and fuel

consumption rates. The designer must then work closely with cost estimators to ensure that each vehicle engine design meets the PM's designated CAIV levels.

When necessary, lessons learned from conducting an AoA could form the basis for modifying one or more key performance parameters (KPPs) of a desired capability. For example, an AoA might produce unacceptably high life cycle costs for all alternatives. Such a result might indicate the originally conceived capability, as reflected in the AoA and KPPs, is driving life cycle cost to the point that achieving the capability is unaffordable. Consequently, it might be necessary to reduce requirements in order to contain life cycle costs at an acceptable level.

Tangential benefits of an AoA include: (a) modeling and simulation inputs for the Test and Evaluation Master Plan (TEMP) and the Life Cycle Management Plan (LCMP), and (b) key information for the ICD.

An AoA analysis is intended to:

- *Enhance and document decision-making by showing the risk, uncertainty, and relative advantages and disadvantages* of the considered alternatives. The WSARA calls for full consideration of all possible trade-offs (cost, schedule, and performance objectives) for each alternative. The analysis should show the sensitivity of each alternative to changes in key assumptions (e.g., threat) or system variables (e.g., selected performance capabilities). Where appropriate, it should include discussion of interoperability and commonality of components/ systems that are functionally similar to other DoD programs or Allied programs. The analysis shall aid decision-makers in judging whether or not any of the proposed alternatives offer sufficient military and/or economic benefit to warrant the cost. There should be a clear linkage between the AoA, capability needs, and MOEs used to evaluate the system.

- *Foster joint ownership and afford a better understanding of subsequent decisions* via early identification and discussion of reasonable alternatives. The analysis should be quantitative in nature, generating discussion of key assumptions and variables.

The AoA will normally include the following sections, although it can (and should) be tailored or streamlined to support the given situation:

- Capability Need, Deficiencies and Opportunities
- Program Description
- Threats
- Operational Environments
- Operational Concept
- Operational Requirements
- Status Quo (Baseline) and Alternatives
- System Design, Performance and Measures of Effectiveness
- Life-Cycle Costs of Baseline and each alternative
- Life Cycle Cost per unit system
- Life Cycle Cost per specified quantity of systems
- Analysis of Alternatives
- Trade-off Analysis
- Sensitivity Analysis

- Conclusions and Recommendations

PREPARATION RESPONSIBILITIES

DoD Instruction 5000.02 establishes the basis for developing an AoA to support milestone and decision reviews. These policies and procedures apply specifically to ACAT I and ACAT IA programs. Component Acquisition Executives (CAEs) may tailor the underlying principles as needed for ACAT II and III programs.

In accordance with Section 201 of WSARA, the OSD Director of Cost Assessment and Program Evaluation (D, CAPE) formulates AoA study guidance for all joint military requirements on which the Chairman of the Joint Requirements Oversight Council (JROC) is the validation authority. Under D, CAPE's cognizance, the DoD Component responsible for the mission area normally prepares the AoA for ACAT I weapon systems. For ACAT IA programs, the OSD Principal Staff Assistant (PSA) office responsible for the functional area to be impacted normally prepares the AoA. The Component Head or PSA is responsible for determining the independent activity to perform the analysis. Pursuant to DoDI 5000.02, the PM may not be designated as the party responsible for performing the AoA.

For potential ACAT ID and ACAT IAM programs (where the milestone decision is made at the DoD level), the Component Head or PSA (as applicable) should coordinate with key OSD officials and staffs early in the AoA process. This coordination is required to increase the likelihood that the full range of alternatives is considered; that organizational and operational plans for the alternatives are consistent with U.S. military strategy; and that joint-service issues such as interoperability, security, and common use are addressed in the AoA.

REVIEWS OF AoAs

An AoA must be prepared and considered for ACAT I and ACAT IA systems at Milestones A, B, and C. The MDA may direct updates to the analysis for subsequent reviews, if conditions warrant. The Defense Acquisition Guidebook (DAG) (available at www.dau.mil) provides discretionary, not prescriptive, best practices and guidance that may be tailored to the needs of each program. The DAG should be used as a complement to regulatory and statutory requirements. The CAE has the authority to decide on the need for, and extent of, AoAs for programs classified as other than ACAT I or ACAT IA.

ACAT I programs: At program initiation, the analysis focuses on broad trade-offs available between a number of different concepts as determined by the MDA. The analysis normally presents a "Go / No Go" recommendation. It demonstrates whether a new system is better than upgrading/modifying an existing system. Cost estimates at this point may be only a rough order of magnitude. However, the affordability of the proposed new system shall be addressed, and an affordability target (initially, average unit acquisition cost and average annual operating and support cost per unit) shall be established which is to be treated by the PM like a KPP. At subsequent milestone reviews, if the AoA is required to be updated, the analysis would be more focused. Hardware alternatives present a more narrow range of choices. The analysis is more detailed than previously as the system is better defined and more cost data are available. Point estimates are given with uncertainty ranges. At the production commitment, an updated AoA is

unlikely to be required unless the program or circumstances (e.g., threat, alliances, operating areas, technology, etc.) have changed significantly.

ACAT IA programs: The AoA for an ACAT IA program will be incorporated into the cost-benefit element structure and process agreed upon by that program's IPT. At program initiation, the Component may conduct a sufficiency review of the PM's life-cycle cost estimate and life-cycle benefits in lieu of a full analysis. Normally, the IPT will establish the content for the sufficiency review. The AoA is usually updated at subsequent milestone reviews in conjunction with the program's life-cycle cost-benefit analysis update.

SERVICE PREPARATION PROCESSES

Each Service conducts the AoA preparation process in its own unique fashion:

Navy: The Office of the Assistant Secretary of the Navy (Research, Development and Acquisition) (ASN (RDA)) released guidance on the preparation of AoAs. An AoA proposal prepared by ASN(RDA) in coordination with the program sponsor, program manager (PM) and appropriate System Command/Program Executive Office initiates the AoA for ACAT I programs. An appointed oversight board frames issues for ASN (RDA) and OP-08/DCS (RP) decision when consensus cannot be readily obtained. A study team prepares the AoA. The PM is represented on the study team and the oversight board. Funding for AoAs is separately identified through the PM with funding from resource sponsors. The PM provides information and support as necessary to the study team.

Air Force: The Air Force Requirements Oversight Council (AFROC) and the Air Force Council review AoAs and draft final results. Either the MAJCOM or the AFROC may request a formal technical assessment by the Technical Review Group (TRG). The AFROC may direct AoA products be presented to the Air Force Group or Board. This action would normally be accomplished to promote advocacy or enhance corporate understanding of the particular program supported by the AoA. If an AoA midterm status report is not required outside of Air Force channels, and the AoA study is proceeding as originally intended in the approved study plan, the study team may request the AFROC waive the requirement to present the midterm status report. AF/XOCA will help the Study Director schedule reviews with the TRG, AFROC, and AF Council. All ACAT I and selected ACAT II study plans, midterm reviews, and final results for Air Force or Joint AoAs, for which the Air Force is the lead service, must have AF/CV approval before being briefed to the OSD working level IPT, Overarching Integrated Product Team (OIPT), or equivalent higher bodies. The AF/CV through AF/CVS is the approval authority for modifications to this review process (e.g., for special access programs). The Department of the Air Force published two documents to provide guidance for conducting an AoA, AFPD 10-6 and AFI 10-601. AFPD 10-6 touches briefing on the Cost and Operational Effectiveness Analysis (COEA) Report which summarizes the cost and performance analyses of the alternatives. The originator, or lead MAJCOM of the new system identifies, explores and evaluates the alternatives and develops requirements in the CDD. AFI 10-601 covers the AoA in more detail.

Army: In the Department of the Army, the Training and Doctrine Command (TRADOC) and the user community bear the responsibility for preparation of the AoA. The PM is a contributor of information and participates in the preparation process. AR 71-9 and the Army Acquisition Handbook provide information on AoA preparation.

SUMMARY

Both the WSARA and DoD Instruction 5000.02 set forth requirements for AoAs, specifically for ACAT I and ACAT IA programs. The AoA is a documented analysis of the performance, operational effectiveness, operational suitability, and estimated costs of alternatives to meet a mission capability, to include assessing the advantages and disadvantages of those various alternatives being considered. An AoA is required early in the defense acquisition process –prior to formal initiation of a program – to ensure that all potential alternative means of satisfying the stated capability are considered. Thereafter, throughout the defense acquisition process, the AoA is either updated or a new one conducted in preparation for the next milestone decision point, depending on then–existing circumstances.

REFERENCES

1. DoD Instruction 5000.02 (Operation of the Defense Acquisition System), 8 December 2008
2. Public Law 111-23, "Weapon Systems Acquisition Reform Act of 2009." 22 May 2009. Available at www.acq.osd.mil/sse/docs/PUBLIC-LAW-111-23-22MAY2009.pdf
3. Directive-Type Memorandum 09-027, "Implementation of the Weapon Systems Acquisition Reform Act of 2009." 4 December 2009.
4. USD(AT&L) Memorandum, "Implementation Directive for Better Buying Power - Obtaining Greater Efficiency and Productivity in Defense Spending." 03 November 2010
5. CJCS Instruction 3170.01G (Joint Capabilities Integration and Development System), 1 March 2009
6. DAU Glossary, 12th Edition, July 2005
7. National Defense Authorization Act for Fiscal Year 2006; House Report 109-089; Section 802 (Requirement for Analysis of Alternatives to Major Defense Acquisition Programs)
8. DoD Extension to "A Guide to the Project Management Body of Knowledge (PMBOK) Guide; First Edition, June 2003
9. Analysis Handbook, A Guide for Performing Analysis Studies: For Analysis of Alternatives or Functional Solution Analyses, Office of Aerospace Studies, July 2004
10. MARCOR Acquisition Procedures Handbook; Section 5 (Analysis of Alternatives – AoA)
11. Analysis of Alternatives Report (template); Defense Finance and Accounting Service, 17 May 2002

THIS PAGE INTENTIONALLY LEFT BLANK

An Overview of CMMC and Process Maturity

The Software Engineering Institute's (SEI) Perspective

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

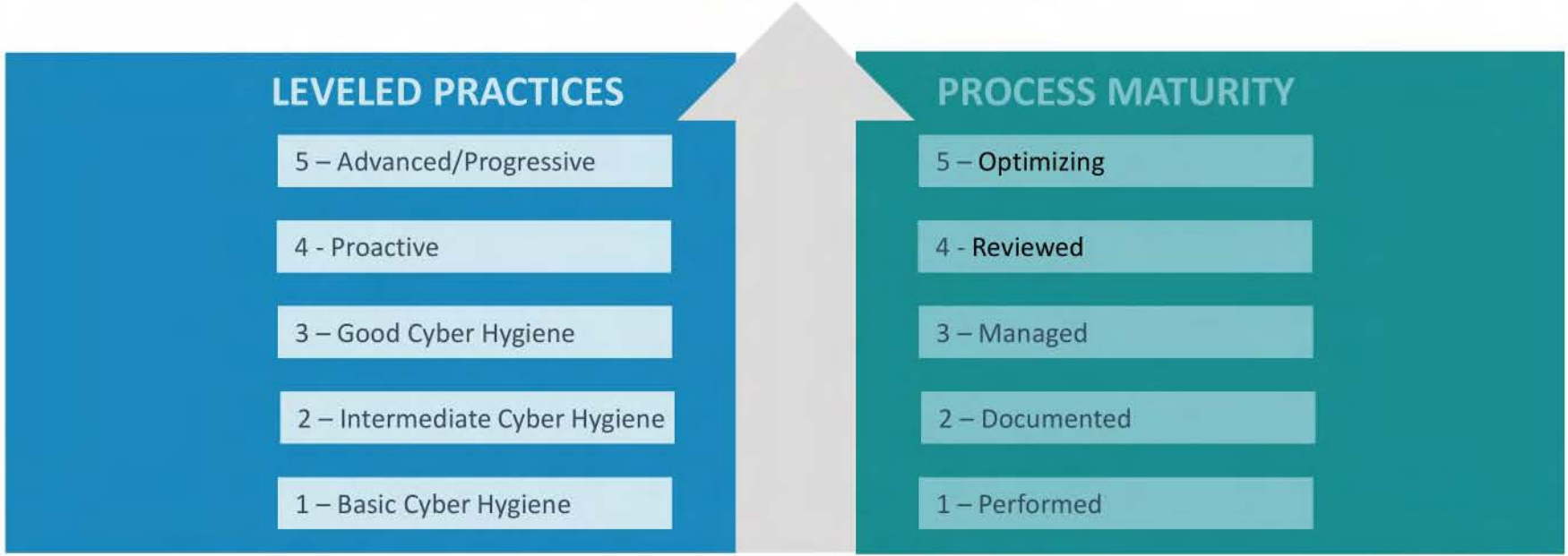
Notices

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM20-0185

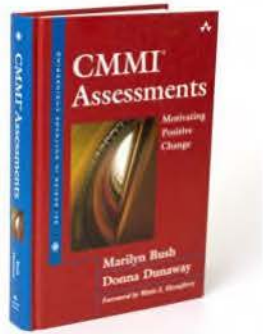
CMMC Model Structure

Organizations are Assessed for Capability and Process Maturity



A Closer Look at Process Maturity

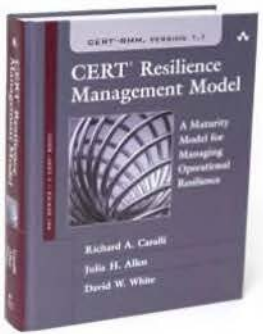
About CMMI and CERT-RMM



Capability Maturity Model Integration (CMMI)

SEI-developed suite of products

- Created for the U.S. Department of Defense
- Assess the quality and capability of DoD software contractors
- Best practices focus on actions for performance improvement, operation alignment to business goals.
- More information: https://cmmiinstitute.com

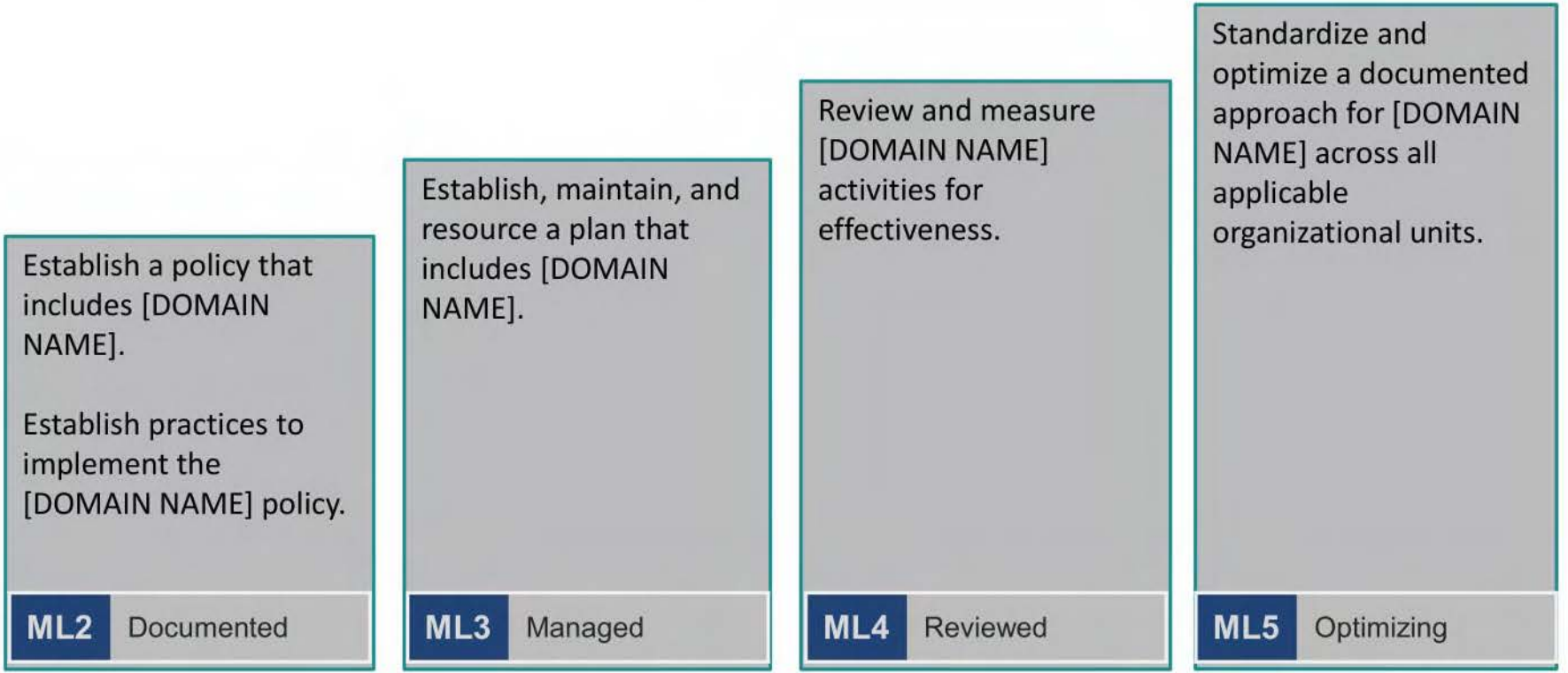


CERT Resilience Management Model (CERT-RMM)

Process improvement approach and CMMC foundational element

- Defines practices to manage operational resilience within an organization
- Proven model that helps organizations respond to cyber events in a mature and predictive manner.
- Publicly available model: cert.org/resilience

CMMC Maturity Processes



How a practice progresses in process maturity

AC.1.001 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

1 Performed	2 Documented	3 Managed	4 Reviewed	5 Optimizing
The organization performs the CMMC practices as defined.	The organization has documented all Access Control practices, and has an Access Control Policy.	The organization has an Access Control Plan that is resourced accordingly.	The organization reviews and measures Access Control activities for effectiveness.	The organization has a standard approach for Access Control, and shares improvements throughout the enterprise.

1 Performed	2 Documented	3 Managed	4 Reviewed	5 Optimizing
The organization performs practices	The organization has	The organization has an	The organization reviews	The organization has a standard approach for Access Control, and shares improvements throughout the enterprise.

1 Performed

Bob is in charge of IT. He assigns everyone a username and password if they are allowed to be on the system. He ensures that everyone can access only what they have permission to access. Bob is performing AC.1.001.

1 Performed

The organization performs practices

2 Documented

The organization has

3 Managed

The organization has an

4 Reviewed

The organization reviews

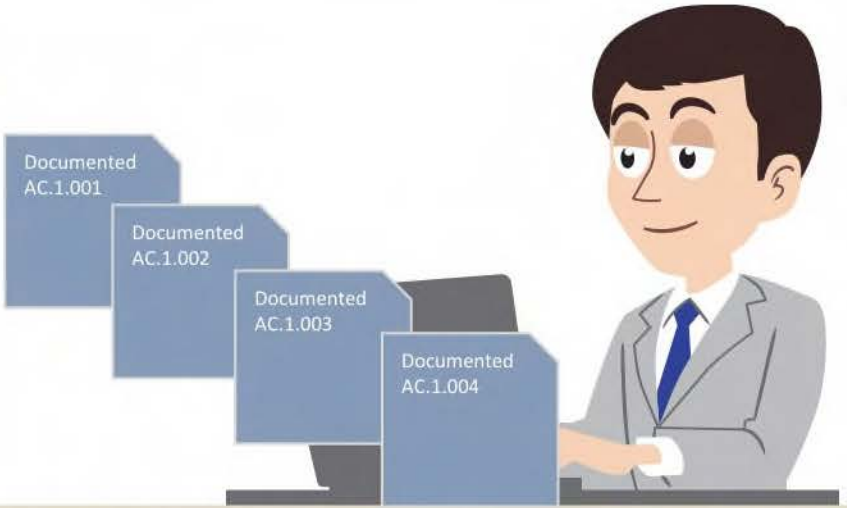
5 Optimizing

The organization has a

2 Documented

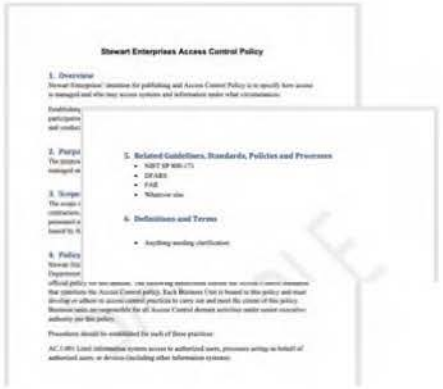
Access Control Policy
- Policy Purpose
- Policy Scope
- Roles and Responsibilities
- Direct establishment of access control procedures
- Regulations guidelines

Documented AC.1.001
- This is my procedure for limiting system access to authorized users.



Senior management recognizes the importance of Access Control, and develops an Access Control Policy. Bob makes sure he is following the Policy. This helps Bob understand the expectations for Access Control at his company, so that he can convey them properly to stakeholders. Bob documents all his Level 1 and Level 2 practices, including AC.1.001. This documentation articulates what needs to be done, so it can be repeated.

ML2 - Policy Examples



One policy written for each CMMC domain

One policy that covers multiple CMMC domains

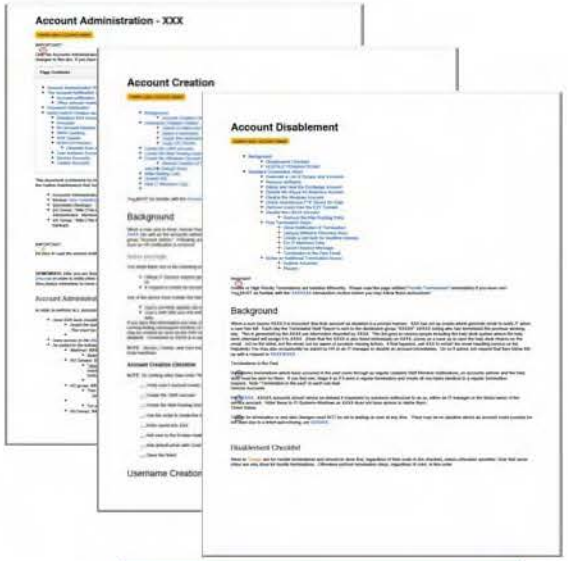
One or more policies that cover all CMMC domains

ML2 - Documented Practices Examples

AC.1.001
Identify users and document them in the notebook per our Access Control policy.
Assign all users a unique username and password.
Limit system access to only authorized users and processes acting on behalf by specify user groups for each of our systems.
Document the user groups into this notebook and make sure users on only allowed to access what they should.
Ensure all system access is limited to authorized devices.
Compare the list of users, processes, and systems that are granted access against the entities of authorized access to ensure we are meeting our Access Control policy.

Handwritten practice documentation

A System Security Plan organized by CMMC Practices



Multiple documented procedures to achieve CMMC practices

1 Performed

The organization performs the practices as

2 Documented

The organization has

3 Managed

The organization has an

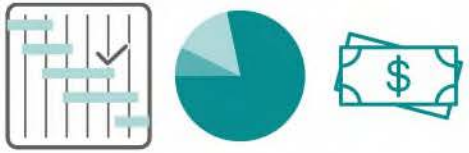
4 Reviewed

The organization reviews

5 Optimizing

The organization has a oach for l, and shares s throughout .

3 Managed



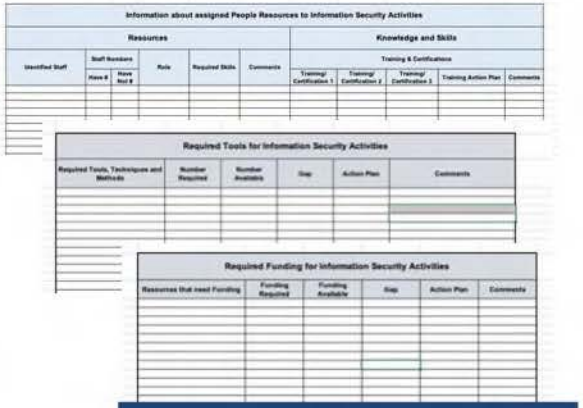
Bob manages his Access Control activities according to a defined plan. The plan defines a mission statement, goals and objectives, required resources and tools, and identified training to achieve the Access Control objectives. Bob makes sure resources are assigned as defined in the plan, which covers all practices for Access Control (including AC.1.001).

Plan Examples

In almost all cases, there will be more than one document to satisfy ML 3

Existing security plans that cover multiple CMMC domains

Project plans can be domain specific or cover the entire scope of CMMC (or beyond)



Resourcing evidence can be domain specific or cover the entire scope of CMMC (or beyond)

1 Performed

The organization performs the practices as

2 Documented

The organization has

3 Managed

The organization has an

4 Reviewed

The organization reviews

5 Optimizing

The organization has a for shares roughout

4 Reviewed

Bob establishes periodic reviews of Access Control activities, which include performance of AC.1.001. For example, he reviews access lists to make sure he disables accounts when responsibilities change or people leave the company. Bob defines and conducts periodic communications with high-level managers to review status, and to inform them of any issues.

Measures and Review Examples

Defined measures, reviews, and reporting will be defined by the organization to meet their improvement objectives

Example metrics for Access control:

- percentage of access requests that adhere to the process policy;
- percentage of access requests approved (based on policy);
- percentage of access requests denied (based on policy);
- number of repeated attempts from the same identity being denied;
- percentage of unapproved access requests that are inappropriate given the requestors
- role or job responsibility; and
- the mean and median time frames between a change in access privileges requiring deprovisioning and the actual deprovisioning.

Example reviews:

- Status reviews of Access Control activities;
- Review of identified issues in process and plan reviews;
- Risks associated with Access Control activities;
- Recommendations for improvements;
- Status or improvements being developed; and
- Schedule for achieving milestones

1 Performed

The organization performs the practices as

2 Documented

The organization has

3 Managed

The organization has an

4 Reviewed

The organization reviews

5 Optimizing

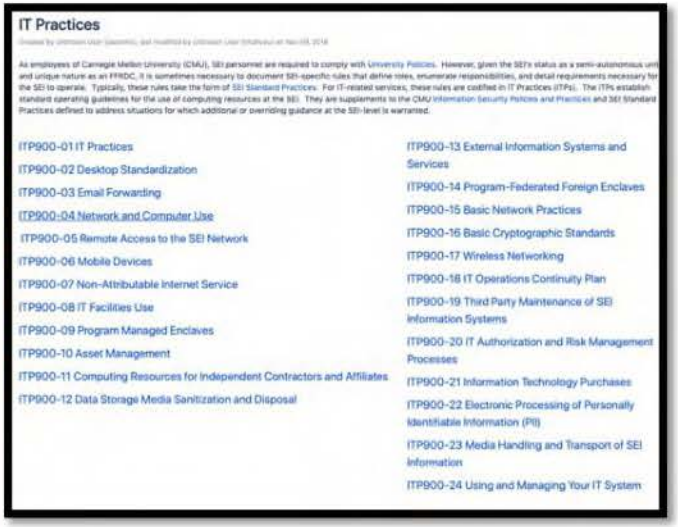
The organization has a

5 Optimizing

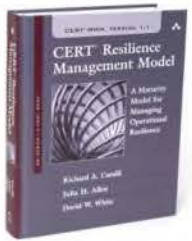
Bob and Sue both do Access Control in different business units within the organization. They develop their procedures, including those for practice AC.1.001, from standard guidance that senior management typically provides. They also communicate and share improvement information they collect when carrying out the Access Control practices, to inform updates to standard guidance.

Standard Process Examples

Documented practices are standardized and shared across the organization



The CERT-RMM Process Area on Organizational Process Definition (OPD) is about establishing and maintaining organizational process assets and work environment standards for operational resilience. https://resources.sei.cmu.edu/asset_files/BookChapter/2016_009_001_514856.pdf

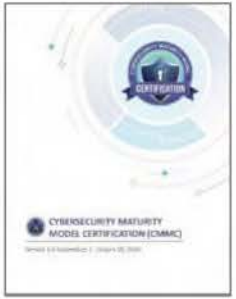


Additional CMMC Information

SEI's CMMC Website

https://www.sei.cmu.edu/go/cmmc

- Blog posts
- Podcasts
- Additional Information
- Contact Information



Model Appendices

https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Appendices_20200203.pdf

- Consolidated Model
- Process and Practice Descriptions
- Glossary
- Abbreviations and Acronyms
- Source Mappings
- References

Accreditation Board (CMMC-AB) Information

https://www.cmmcab.org/

- Register for email list
- Working Group Information
- Current accreditation information

CMMC Status

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

- Authoritative source for model documents and updates
- Authoritative source for assessment guidance
- Authoritative source for CMMC model updates

Contact Us

Katie Stewart
kcstewart@cert.org

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

412 268 5800

https://www.sei.cmu.edu/