Presented By:

The Georgia Defense Industrial Base Task Force

In cooperation with:

TAG
Technology Association of Georgia

Georgia®
USA

Georgia Department of Economic Development

This material is intended to be informational and does not constitute legal or other advice. Please consult your advisor for advice specific to your situation.

Understanding CMMC

Level 1 Certification

Mark Lupo, MBA, MBCP, SMP

The University of Georgia

Small Business Development Center

July 28, 2020

Overview

I. Background

II.Requirements

III.Compliance

IV.CMMC

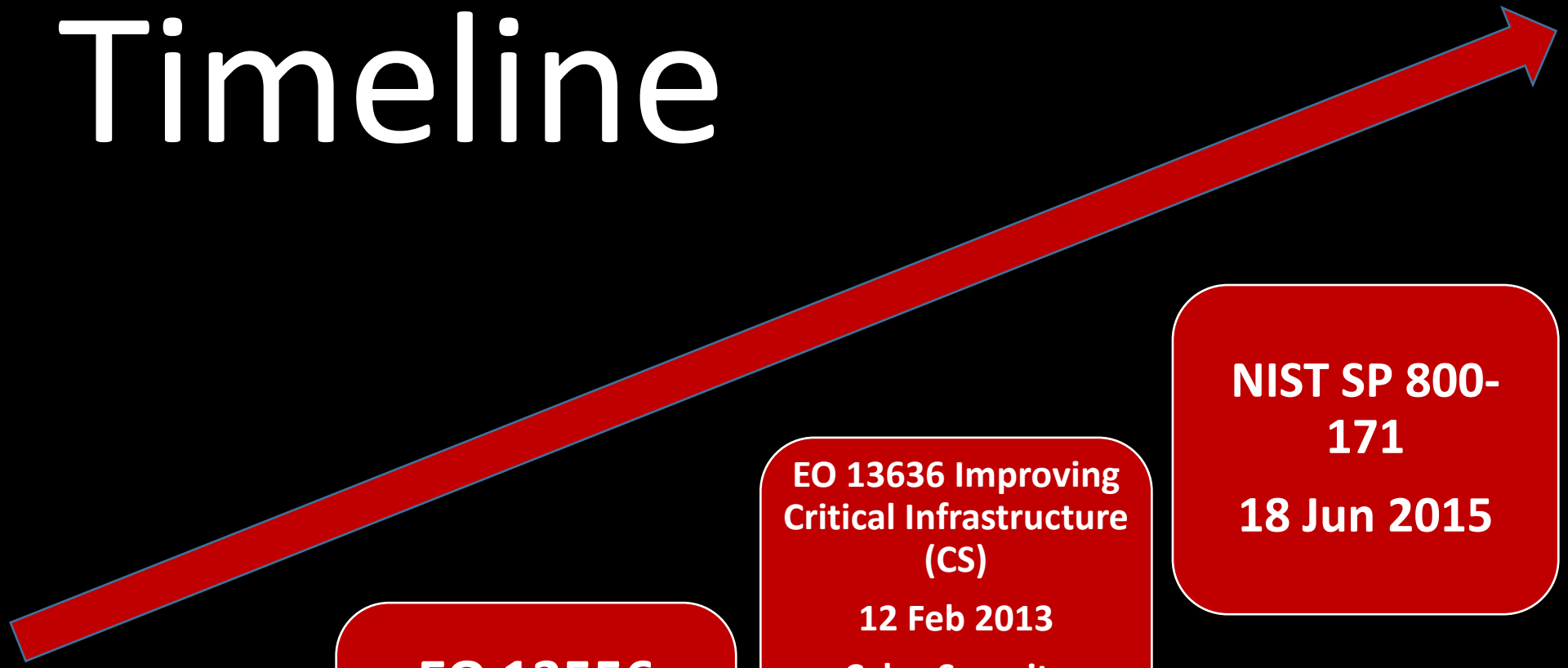
Cybersecurity and Supply Chain Risk Management

STARS III bidders will be considered in light of the terms and conditions of as many as 38 cybersecurity and supply chain risk management (SCRM) laws, regulations, standards and policies listed in an attachment document to the RFP.

The RFP addresses the possibility that some STARS III task orders will be subject to the Pentagon's contentious Cybersecurity Maturity Model Certification (CMMC) that requires all defense suppliers to undergo regular cybersecurity audits. It's likely the initiative will soon extend to all agencies. The RFP instructs companies to "begin preparing for CMMC and SCRM accreditation by staying aware of developing requirements." Although non-compliant CMMC companies will not be disqualified for a STARS III bid, but Bloomberg Government expects it may put companies at a competitive disadvantage for task orders in future years.

Background

Timeline



NIST SP 800-53
Initial Release
Dec 2005

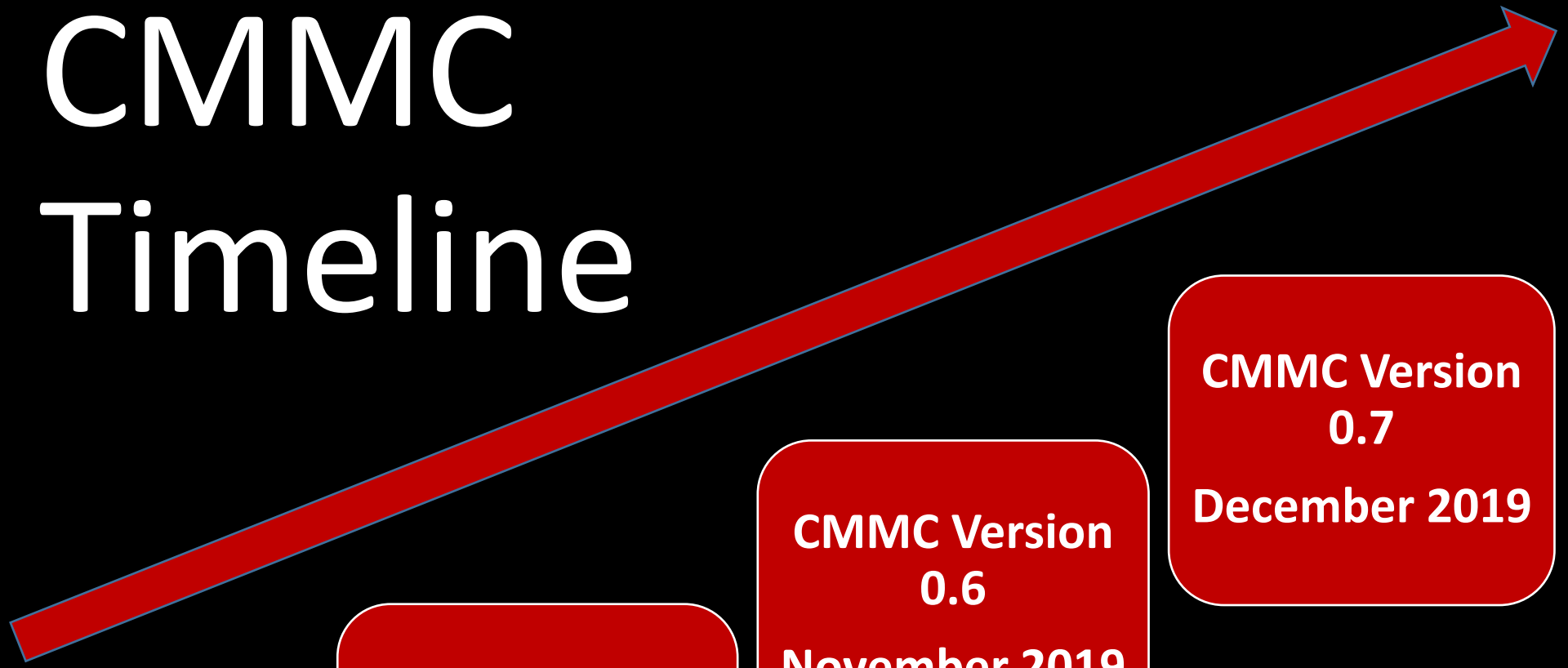
EO 13556 (CUI)
4 Nov 2010

EO 13636 Improving Critical Infrastructure (CS)
12 Feb 2013
CyberSecurity Framework

NIST SP 800-171
18 Jun 2015

NIST SP 800-171
Full Compliance Mandated
31 Dec 2017
Rev 1 – 20 Feb 2018

CMMC Timeline



CMMC Version 0.3

June 2019

CMMC Version 0.4

September 2019

CMMC Version 0.6

November 2019

CMMC Version 0.7

December 2019

CMMC Version 1.0

January 2020

Small Business Development Center
UNIVERSITY OF GEORGIA

The CyberSecurity Framework

Small Business Development Center
UNIVERSITY OF GEORGIA

Requirements

Primary Trigger - DFARS Clause

(DFARS) **252.204-7012**

(Safeguarding of Unclassified, Controlled Technical Information)

- This clause triggers compliance requirements to NIST SP 800-171, Rev 2

Small Business Development Center
UNIVERSITY OF GEORGIA

NIST SP 800-171 (Rev 2)

- 14 Families of Security Requirements

14 Families of Security Requirements

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

NIST SP 800-171 (Rev 2)

- 14 Families of Security Requirements
- 110 Control Points
- System Security Plan (SSP) and Plan of Action and Milestones (POAM)
- Need a Breach Response Plan

When Present, Must Either…

- Not bid on the contract
- Take steps to comply with the information security requirements covered within NIST SP 800-171, Rev 2
- Seek an exception to the application of the rule
- Disclose and request approval of an alternative, but equally effective, security measure that may be implemented in place of compliance with requirements.

Some Definitions…

- Defense Industrial Base (DIB)
- Covered Defense Information (CDI)
- Federal Contract Information (FCI)
- Controlled, Unclassified Information (CUI)
- Code of Federal Regulations (CFR)
- Defense Contract Management Agency (DCMA)
- Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)

37--Lawn Mower

Solicitation Number: POLKDPTMSMC0005
Agency: Department of the Army
Office: FedBid
Location: FedBid.com -- for Department of Army procurements only

Original Synopsis
Aug 29, 2018
11:36 am

Solicitation Number: POLKDPTMSMC0005
Notice Type: Combined Synopsis/Solicitation

Synopsis:
Added: Aug 29, 2018 11:36 am
This is a combined synopsis/solicitation for commercial items prepared in accordance with the format in FAR Subpart 12.6, as supplemented with additional information included in this notice. The solicitation number is POLKDPTMSMC0005 and is issued as an invitation for bids (IFB), unless otherwise indicated herein. The solicitation document and incorporated provisions and clauses are those in effect through Federal Acquisition Circular 2005-100. The associated North American Industrial Classification System (NAICS) code for this procurement is 333112 with a small business size standard of 500.00 employees. This requirement is a [Small Business] set-aside and only qualified offerors may submit bids. The solicitation pricing on www.FedBid.com will start on the date this solicitation is posted and will end on 2018-09-05 11:00:00.0 Eastern Time or as otherwise displayed at www.FedBid.com. FOB Destination shall be FORT POLK, LA 71459

The MICC End User requires the following items, Brand Name or Equal, to the following:
LI 001: 96L X 86 W (IN), Z997R Commercial L.C. Diesel Max-Frame Zero-Turn-Radius Mower or equal. With 72" side discharge 7-iron PRO deck. Mfr Part No: 0911TC. Standard Warranty. Made in the USA. Weight: 1845.000 LB., 1, EA;

Solicitation and Buy Attachments

***Question Submission: Interested offerors must submit any questions concerning the solicitation at the earliest time possible to enable the Buyer to

GENERAL INFORMATION

Notice Type:
Combined Synopsis/Solicitation

Posted Date:
August 29, 2018

Response Date:
September 5, 2018

Archiving Policy:
Automatic, on specified date

Archive Date:
March 4, 2019

Original Set Aside:
N/A

Set Aside:
Total Small Business

Classification Code:
37 -- Agricultural machinery & equipment

Office of Command Counsel
4400 Martin Road
Rm: A6SE040.001
Redstone Arsenal, AL 35898-5000
Fax: (256) 450-8840
Packages sent by FedEx or UPS should be addressed to:
Headquarters U.S. Army Materiel Command
Office of Command Counsel
4400 Martin Road
Rm: A6SE040.001
Redstone Arsenal, AL 35898-5000
Fax: (256) 450-8840 The AMC-Level Protest procedures are found at:
http://www.amc.army.mil/pa/COMMANDCOUNSEL.asp.
If internet access is not available, contact the contracting officer or HQ, AMC to obtain the HQ AMC-Level Protest Procedures."

"52.204-9, Personal Identity Verification of Contractor Personnel; 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards; 52.222-41, Service Contract Act; 52.237-2, Protection of Government Buildings, Equipment and Vegetation; 252.201-7000, COR Clause; 252.223-7006,
Prohibition On Storage And Disposal Of Toxic And Hazardous Materials; 252.243-7001, Pricing of Contract Modifications; 252.246-7000, Material inspection and receiving report"

Representation by Corporations Regarding an Unpaid Tax Liability or a Felony Conviction under any Federal Law.

Wide Area WorkFlow Payment Instructions

252.204-7012 Safeguarding of Unclassified Controlled Technical Information

All deliveries shall be palletized when the material exceeds 250 lbs. (excluding the pallet), or exceeds 20 cubic feet, to comply with the requirements of Department of the Army Pamphlet 700-32 and MIL-STD-147E.

This is currently an unfunded requirement with a high expectation that funds will be available. When and if funds become available a contract will be awarded at that time.

Please address your questions through the FedBid buy. If your questions are not being answered in a timely manner, please send your question to the S2P2 Contracting Officer - usarmy.drum.acc-micc.mbx.micc@mail.mil or call 315-772-5582.

Additional Info:
www.fedbid.com (b-945655, n-252513)

84--Firefighter Turnout Gear GLOBE EXCEL

ACTIVE

Contract Opportunity

Notice ID
BUCHANANDESWM2009

Related Notice

Department/Ind. Agency
DEPT OF DEFENSE
Sub-tier
DEPT OF THE ARMY
Major Command
AMC
Sub Command
ACC
Sub Command 2
MISSION & INSTALLATION CONTRACTING COMMAND
Sub Command 3
419TH CSB
Office
W6QM MICC-FT DRUM

General Information

Contract Opportunity Type: Combined Synopsis/Solicitation (Original)
All Dates/Times are: (UTC-04:00) EASTERN STANDARD TIME, NEW YORK, USA
Original Published Date: Jul 17, 2020 01:42 pm EDT
Original Date Offers Due: Jul 22, 2020
Inactive Policy: Manual
Original Inactive Date: Jan 18, 2021

However, you can also protest to Headquarters (HQ), Army Materiel Command (AMC). The HQ AMC-Level Protest Program is intended to encourage interested parties to seek resolution of their concerns within AMC as an Alternative Dispute Resolution forum, rather than filing a protest with the Government Accountability Office (GAO) or other external forum. Contract award or performance is suspended during the protest to the same extent, and within the same time periods, as if filed at the GAO. The AMC protest decision goal is to resolve protests within 20 working days from filing. To be timely, protests must be filed within the periods specified in FAR 33.103. If you want to file a protest under the HQ AMC-Level Protest Program, the protest must request resolution under that program and be sent to the address below. All other agency-level protests should be sent to the contracting officer for resolution. Headquarters U.S. Army Materiel Command Office of Command Counsel 4400 Martin Road Rm: A6SE040.001 Redstone Arsenal, AL 35898-5000 Fax: (256) 450-8840 Packages sent by FedEx or UPS should be addressed to: Headquarters U.S. Army Materiel Command Office of Command Counsel 4400 Martin Road Rm: A6SE040.001 Redstone Arsenal, AL 35898-5000 Fax: (256) 450-8840 The AMC-Level Protest procedures are found at: http://www.amc.army.mil/pa/COMMANDCOUNSEL.asp. If internet access is not available, contact the contracting officer or HQ, AMC to obtain the HQ AMC-Level Protest Procedures."

"52.204-9, Personal Identity Verification of Contractor Personnel; 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards; 52.222-41, Service Contract Act; 52.237-2, Protection of Government Buildings, Equipment and Vegetation; 252.201-7000, COR Clause; 252.223-7006, Prohibition On Storage And Disposal Of Toxic And Hazardous Materials; 252.243-7001, Pricing of Contract Modifications; 252.246-7000, Material inspection and receiving report"

Representation by Corporations Regarding an Unpaid Tax Liability or a Felony Conviction under any Federal Law.

Wide Area WorkFlow Payment Instructions

252.204-7012 Safeguarding of Unclassified Controlled Technical Information

All deliveries shall be palletized when the material exceeds 250 lbs. (excluding the pallet), or exceeds 20 cubic feet, to comply with the requirements of Department of the Army Pamphlet 700-32 and MIL-STD-147E.

Assault Breacher Vehicle Remote Control System Market Survey

What you think matters!

Provide Feedback

ACTIVE

Contract Opportunity

Notice ID
PANDTA-20-P-0000-008592

Related Notice

Department/Ind. Agency
DEPT OF DEFENSE
Sub-tier
DEPT OF THE ARMY
Major Command
AMC
Sub Command
ACC
Sub Command 2
ACC-CTRS
Sub Command 3
ACC WRN
Office
W4GG HQ US ARMY TACOM

General Information

View Changes

Contract Opportunity Type: Sources Sought (Updated)
All Dates/Times are: (UTC-04:00) EASTERN STANDARD TIME, NEW YORK, USA
Updated Published Date: Jul 09, 2020 02:17 pm EDT
Original Published Date: Jun 02, 2020 02:14 pm EDT
Updated Response Date: Jul 13, 2020 01:00 pm EDT
Original Response Date: Jul 02, 2020 01:00 pm EDT
Inactive Policy: 15 days after response date
Updated Inactive Date: Jul 28, 2020
Original Inactive Date: Jul 17, 2020

Contract Opportunity
General Information
Classification
Description
Attachments/Links
Contact Information
History

What you think matters!

Provide Feedback

Classification

Original Set Aside:
Product Service Code: 2350 - COMBAT, ASSAULT, AND TACTICAL VEHICLES, TRACKED
NAICS Code: 334511 - Search, Detection, Navigation, Guidance, Aeronautical, and Nautical System and Instrument Manufacturing
Place of Performance:

Description

View Changes

Market Survey Questionnaire

Assault Breacher Vehicle Remote Control System

DESCRIPTION OF INTENT:

THIS IS A MARKET INVESTIGATION REQUESTING INFORMATION IN SUPPORT OF THE FOLLOWING PERFORMANCE REQUIREMENTS: No contract will be awarded from this announcement. This is not a Request for Proposal (RFP) or an announcement of a forthcoming solicitation. Also, it is not a request seeking contractors interested in being placed on a solicitation mailing list. Response to this questionnaire is voluntary and no reimbursement will be made for any costs associated with providing information in response to the market survey and any follow-on information requests. Data submitted in response to this market investigation will not be returned. Although no solicitation document exists at this time, information derived from this market investigation will help the Government determine the suitability of the marketplace for satisfying this performance requirement. This requirement is a candidate for a CMMC pilot program. Any resulting contract may exercise the CMMC process as a non-attribution, not-for-credit assessment of the prime contractor and select subcontractors as part of the scope of work.

Contract Opportunity

General Information

Classification

Description

Attachments/Links

Contact Information

History

What you think matters!

Provide Feedback

Manuals(TM)? What is the assumed number of total work packages or total pages in a Technical Manual (TM)?

22. Does your company have any experience in participating/executing Logistics events such as Provisioning Conferences, Logistics Demonstrations and TM Verifications or Logistics Integrated Program Reviews related to the areas of Training Development, Publications Development, and maintenance development?

23. Have you ever been required by a Federal contract, subcontract, solicitation, or agreement to transmit, store, or process federal contract information on nonfederal information systems and comply with the FAR Clause 52.204-21? If so, which of the NIST SP 800-171 requirements have not been met, if any? Have you ever been required by a DoD contract, subcontract, solicitation, or agreement to transmit, store, or process controlled unclassified information (CUI) on nonfederal information systems and comply with the DFARS clause 252.204-7012? If so, which of the NIST SP 800-171 requirements have not been met, if any? Has your system security plan (SSP) ever been assessed by the DCMA DIBCAC? If so, what score did it receive? How many (or percentage) of your potential subcontractors have ever been required to comply with FAR clause 52.204-21? DFARS clause 252.204-7012? How many (or percentage) of subcontractors are expected to transmit, store, or process FCI or CUI in the performance of this contract, if any? How many or what percentage of your potential subcontractors have SSPs that have been assessed by the DCMA DIBCAC?

24. Please provide any information you believe we are missing or are overlooking.

Compliance

Step 1: Determine the Scope of the Contract
Step 2: Assess Level of Compliance
Step 3: Clarify Plan of Action/Milestones
Step 4: Develop System Security Plan
Step 5: Ongoing Compliance Initiatives

What is a maturity model?

- A tool for assessing an organization's effectiveness at achieving a particular goal.
- Enables organizations to identify where their practices are weak or not taken seriously and where their practices are truly embedded.
- Help to distinguish between organizations in which security is *baked in* and those in which it is merely *bolted on*.
- Gives an organization’s leadership a way to measure the progress made in embedding security into its day-to-day and strategic operations.

National Cyber Security Centre – Ann W

CyberSecurity Maturity Model Certification (CMMC)

- CMMC requires a third party, cybersecurity certification to validate the cybersecurity infrastructure of the company

C3PAO | Assessors | Registered Provider Organization | Registered Practitioners | Organizations Seeking Certification | Government Agencies COMING SOON | Licensed Instructors COMING SOON | Licensed Publishing Partner | Licensed Training Providers COMING SOON | CMMC-AB Staff COMING SOON

C3PAO

Certified Third-Party Assessor Organization

Contract with OSCs
Connect with Organizations Seeking Certification on the CMMC-AB Marketplace

Schedule Assessments
Schedule assessments on the CMMC-AB portal

Hire and Train Certified Assessors
Only Certified Assessors supported by Certified Professionals may deliver assessments

Manage Assessments
Deliver assessments with Certified Assessor led teams to contracted clients and provide advisory services to other OSCs

A C3PAO authorized to manage the assessment process.

The CMMC-AB estimates that up to 6,000 companies will require CMMC certification in Federal FY21 https://www.cmmcab.org/c3pao-lp

Washingtontechnology.com

CyberSecurity Maturity Model Certification (CMMC)

- CMMC requires a third party, cybersecurity certification to validate the cybersecurity infrastructure of the company
- Will grade cybersecurity infrastructure on a scale of 1 to 5, 5 being the most stringent
- Standards defined as of January 2020
- Certifying companies are being trained and ‘certified’ by summer of 2020.
- Approximately 300,000+ DOD contractors will need to be certified
- Contract solicitations (RFP’s) will begin incorporating CMMC requirements (#1 to #5) in September of 2020
- Will require a company, Tier 1 and subs, to have the CMMC certification to match the level required on the solicitation prior to being awarded the contract

CMMC Model Framework

Domains — 17 Categories for cybersecurity

Capabilities — 43 Achievements to ensure cybersecurity within each domain

Practices and Processes — Activities required by level to achieve a capability (total of 171)

Small Business Development Center
UNIVERSITY OF GEORGIA

Carnegie Mellon University/Johns Hopkins University

CMMC
17 Domains

Figure 3. CMMC Model Domains

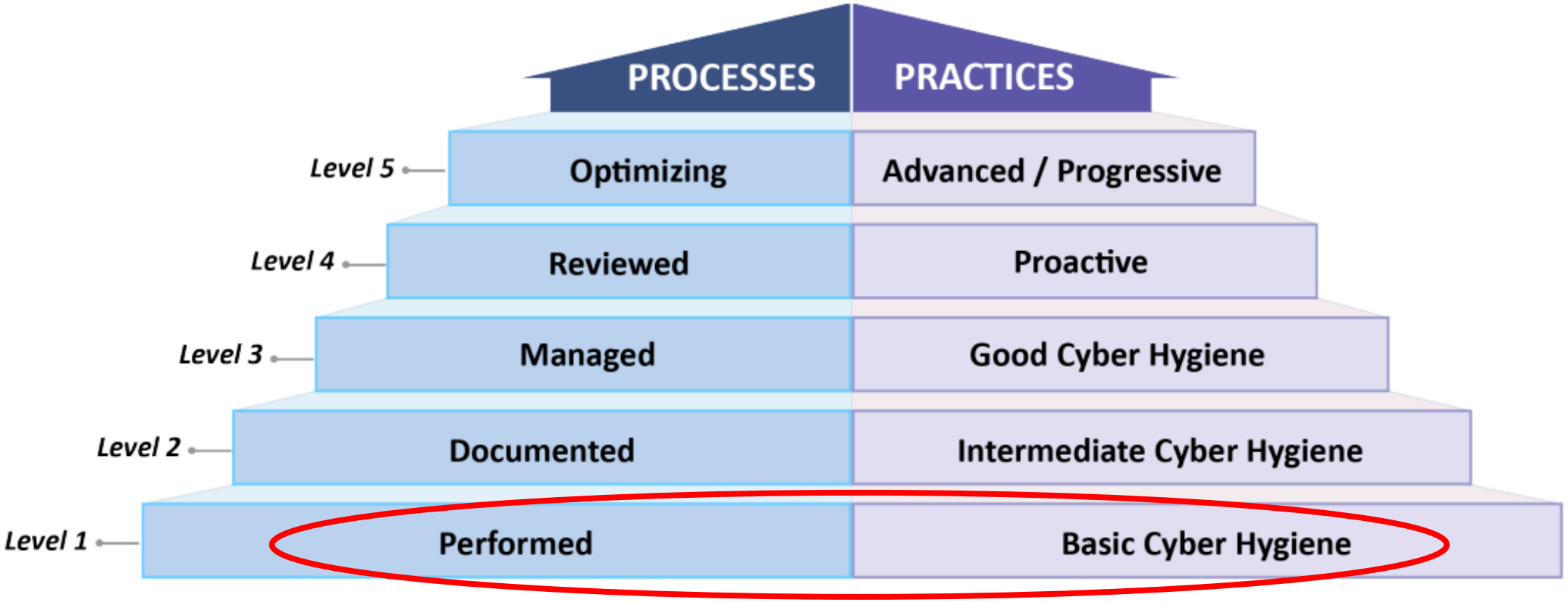


Figure 2. CMMC Levels and Descriptions

CMMC Practices Per Level

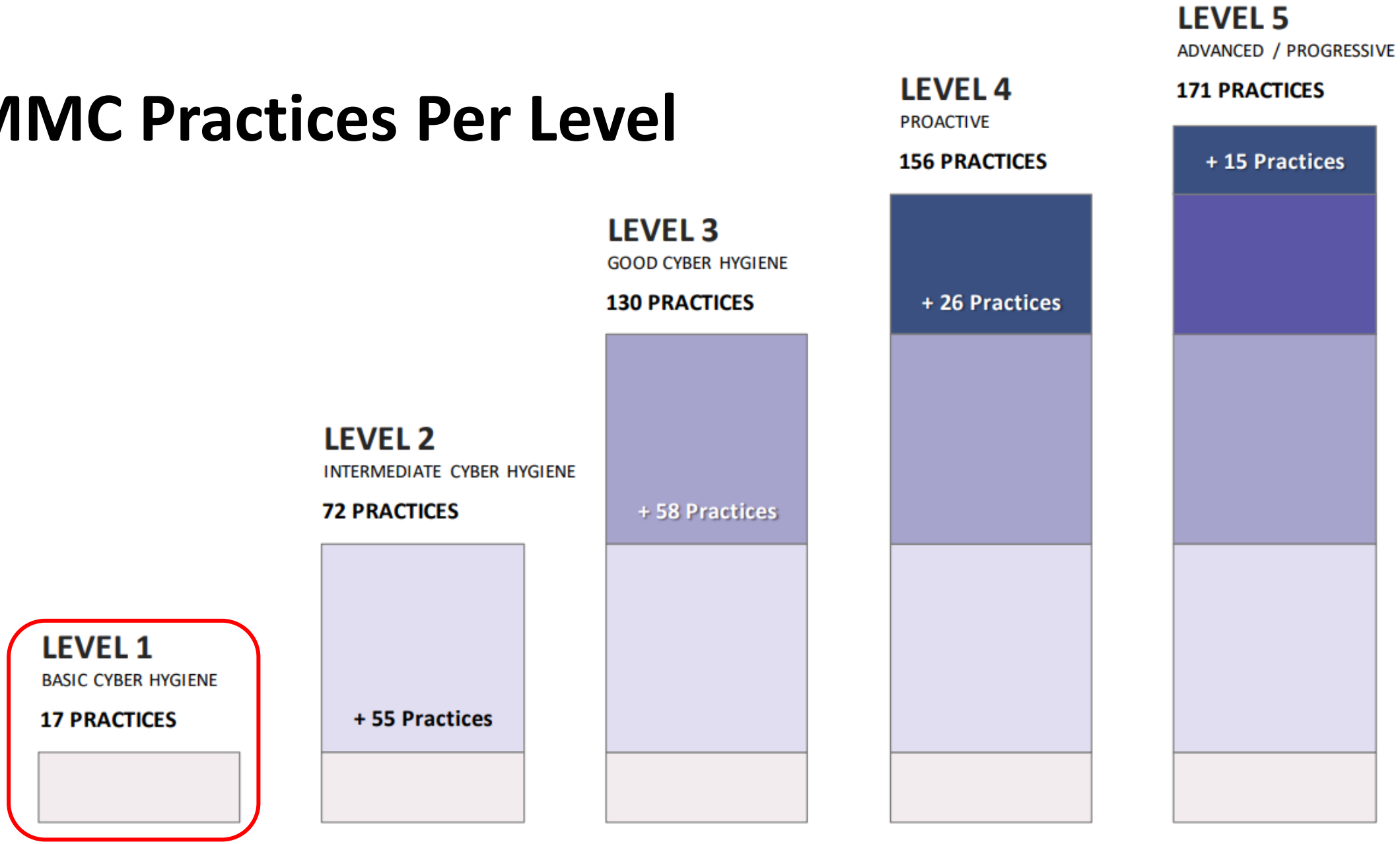


Figure 5. CMMC Practices Per Level

48 CFR § 52.204-21

Basic Safeguarding of Covered Contractor Information Systems

- The Basis for CMMC Level 1 Compliance
- Consists of 17 Practices

48 CFR § 52.204-21

Basic Safeguarding of Covered Contractor Information Systems

I. Domain – Access Control (AC)
3 Capabilities, 4 Practices

II. Domain – Identification and Authentication (IA)
1 Capability, 2 Practices

III. Domain – Media Protection (MP)
1 Capability, 1 Practice

IV. Domain – Physical Protection (PE)
1 Capability, 4 Practices

V. Domain – System and Communication Protections (SC)
1 Capability, 2 Practices

VI. Domain – System and Information Integrity (SI)
2 Capabilities, 4 practices

Small Business Development Center
UNIVERSITY OF GEORGIA

Office of the Under Secretary of Defense for
Acquisition & Sustainment
Cybersecurity Maturity Model Certification

Search

Home | Updates | FAQ's | CMMC Model | Contact Us

CMMC Model overview briefing:

CMMC Model Briefing PDF

CMMC Model v1.02:

CMMC Model PDF

CMMC Model v1.02 Appendices:

CMMC Model Appendices PDF

CMMC Model v1.02 (Appendix A) in tabular format:

CMMC Model (Appendix A) Excel

CMMC Model Errata:

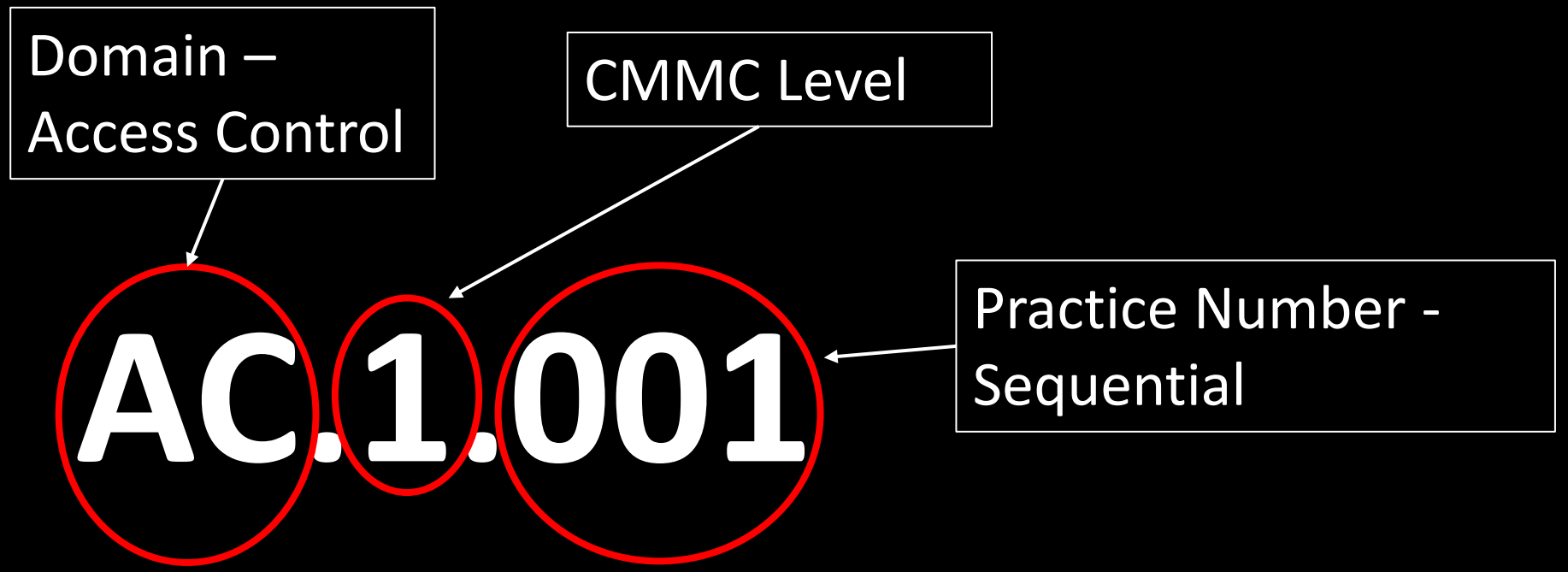
CMMC Model Errata PDF

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

CMMC V1.02 Appendices

- **Appendix A – CMMC V1.0 Model Overview (Pg. 6 – 40)**
- **Appendix B – Process and Practice Descriptions (Pg. 41 – 295)**
- **Appendix C – Glossary (Pg. 296 – 322)**
- **Appendix D – Abbreviations and Acronyms (Pg. 323 – 324)**
- **Appendix E – Source Mapping (Pg. 325 – 332)**
- **Appendix F – References (Pg. 333 – 337)**

Small Business Development Center
UNIVERSITY OF GEORGIA



Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and is numbered with the reference number.

ACCESS CONTROL (AC)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C001 Establish system access requirements	AC.1.001 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). • FAR Clause 52.204-21 b.1.i • NIST SP 800-171 Rev 1 3.1.1 • CIS Controls v7.1 1.4, 1.6, 5.1, 14.6, 15.10, 16.8, 16.9, 16.11 • NIST CSF v1.1 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4 • CERT RMM v1.2 TM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-2, AC-3, AC-17 • AU ACSC Essential Eight	AC.2.005 Provide privacy and security notices consistent with applicable CUI rules. • NIST SP 800-171 Rev 1 3.1.9 • NIST SP 800-53 Rev 4 AC-8			
		AC.2.006 Limit use of portable storage devices on external systems. • NIST SP 800-171 Rev 1 3.1.21 • CIS Controls v7.1 13.7, 13.8, 13.9 • NIST CSF v1.1 ID.AM-4, PR.PT-2 • NIST SP 800-53 Rev 4 AC-20(2)			

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C002 Control internal system access	AC.1.002 Limit information system access to the types of transactions and functions that authorized users are permitted to execute. • FAR Clause 52.204-21 b.1.ii • NIST SP 800-171 Rev 1 3.1.2 • CIS Controls v7.1 1.4, 1.6, 5.1, 8.5, 14.6, 15.10, 16.8, 16.9, 16.11 • NIST CSF v1.1 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4 • CERT RMM v1.2 TM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-2, AC-3, AC-17	AC.2.007 Employ the principle of least privilege, including for specific security functions and privileged accounts. • NIST SP 800-171 Rev 1 3.1.5 • CIS Controls v7.1 14.6 • NIST CSF v1.1 PR.AC-4 • CERT RMM v1.2 KIM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-6, AC-6(1), AC-6(5) • UK NCSC Cyber Essentials	AC.3.017 Separate the duties of individuals to reduce the risk of malevolent activity without collusion. • NIST SP 800-171 Rev 1 3.1.4 • NIST CSF v1.1 PR.AC-4 • NIST SP 800-53 Rev 4 AC-5	AC.4.023 Control information flows between security domains on connected systems. • CMMC modification of Draft NIST SP 800-171B 3.1.3e • CIS Controls v7.1 12.1, 12.2, 13.1, 13.3, 14.1, 14.2, 14.5, 14.6, 14.7, 15.6, 15.10 • NIST CSF v1.1 ID.AM-3, PR.AC-5, PR.DS-5, PR.PT-4, DE.AE-1 • NIST SP 800-53 Rev 4 AC-4, AC-4(1), AC-4(6), AC-4(8), AC-4(12), AC-4(13), AC-4(15), AC-4(20)	AC.5.024 Identify and mitigate risk associated with unidentified wireless access points connected to the network. • CMMC • CIS Controls v7.1 15.3 • NIST CSF v1.1 PR.DS-5, DE.AE-1, DE.CM-7 • NIST SP 800-53 Rev 4 SI-4(14)
		AC.2.008 Use non-privileged accounts or roles when accessing nonsecurity functions. • NIST SP 800-171 Rev 1 3.1.6 • CIS Controls v7.1 4.3, 4.6 • NIST CSF v1.1 PR.AC-4 • NIST SP 800-53 Rev 4 AC-6(2) • UK NCSC Cyber Essentials	AC.3.018 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. • NIST SP 800-171 Rev 1 3.1.7 • NIST CSF v1.1 PR.AC-4 • CERT RMM v1.2 KIM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-6(9), AC-6(10)	AC.4.025 Periodically review and update CUI program access permissions. • CMMC	
		AC.2.009 Limit unsuccessful logon attempts. • NIST SP 800-171 Rev 1 3.1.8 • NIST CSF v1.1 PR.AC-7 • NIST SP 800-53 Rev 4 AC-7	AC.3.019 Terminate (automatically) user sessions after a defined condition. • NIST SP 800-171 Rev 1 3.1.11 • CIS Controls v7.1 16.7, 16.11 • NIST SP 800-53 Rev 4 AC-12		
		AC.2.010 Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity. • NIST SP 800-171 Rev 1 3.1.10 • CIS Controls v7.1 16.11 • NIST SP 800-53 Rev 4 AC-11, AC-11(1)	AC.3.012 Protect wireless access using authentication and encryption. • NIST SP 800-171 Rev 1 3.1.17 • CIS Controls v7.1 15.7, 15.8 • NIST CSF v1.1 PR.PT-4 • CERT RMM v1.2 KIM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-18(1)		

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

CMMC Practice Description

DISCUSSION FROM SOURCE: DRAFT NIST SP 800-171 R2

Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses non-privileged) are addressed in requirement 3.1.2 (AC.1.002).

Discussion and content description of the Practice from NIST SP 800-171, R2

CMMC CLARIFICATION

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.

Example 1

You are in charge of 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 only to those employees you know have permission to be on the system. When an employee leaves the company, you disable their username and password immediately.

Example 2

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.

Clarification with Examples

REFERENCES

References

Process to Move Forward

- Assess compliance to NIST SP 800-171, Rev 2
- Develop SSP and POAM
- Determine compliance to CMMC Level 1
  - Either internal or external assessment initially
- Move to comply with all Level 1 requirements
- Once implemented, have external assessment completed
- Move toward certification to CMMC Level 1 compliance

The Georgia Defense Industrial Base (GDIB) Task Force is here to help!

Resources:

Georgia Defense Industrial Base Task Force: https://www.tagonline.org/ga-dibt/

Georgia Department of Economic Development – Cybersecurity EDGE Program: https://www.georgia.org/cybersecurityedge

CMMC-AB Website: https://www.cmmcab.org

Department of Defense: https://www.acq.osd.mil/cmmc/index.html

The University of Georgia SBDC

"The Trusted Resource for Transforming Georgia Businesses"

Small Business Development Center
UNIVERSITY OF GEORGIA

Mark R. Lupo, MBA, MBCP, SMP
706-542-2762
mlupo@georgiasbdc.org
https://www.linkedin.com/in/marklupo