



# Set Up To Fail?

Cybersecurity Compliance in the Last Mile of the DoD Supply Chain

# AGENDA

## Timeline

The CUI Rule

NIST SP 800-171

DFARS 252.204-7012

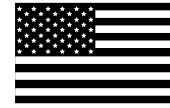
## The Last Mile

## CMMC Implications

## Key Takeaways & Next Steps

# HOW WE GOT HERE

**November 2002**



**Homeland Security Act**

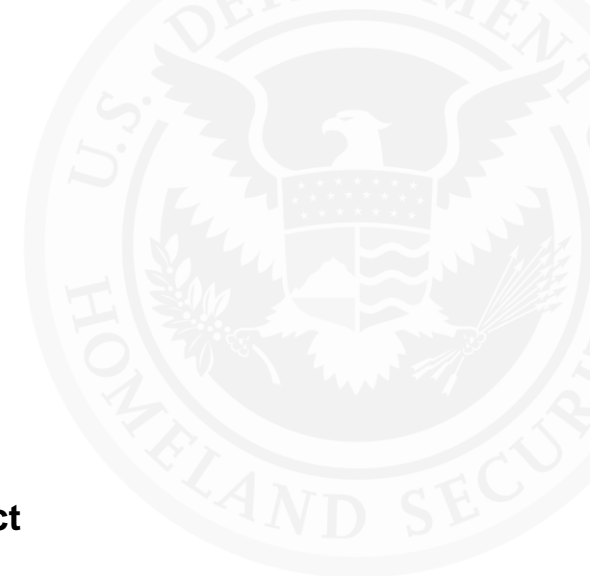
*"...identify and safeguard homeland security information that is Sensitive But Unclassified (SBU)."*

**Intelligence Reform & Terrorism Prevention Act**

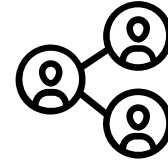
*"...facilitate the sharing of terrorism information ... at and across all levels of security."*



**December 2004**



**December 2005**



**Presidential Memorandum**

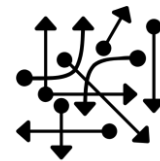
*"Guidelines & Requirements in Support of the Information Sharing Environment."*

**Presidential Memorandum**

*"Designation & Sharing of Controlled Unclassified Information (CUI)."*



**May 2008**



**Presidential Memorandum**

*"Classified Information & Controlled Unclassified Information."*

**May 2009**



## Presidential Task Force on CUI Report

*"...a single, standardized framework for marking, safeguarding, and disseminating [CUI] is required..."*



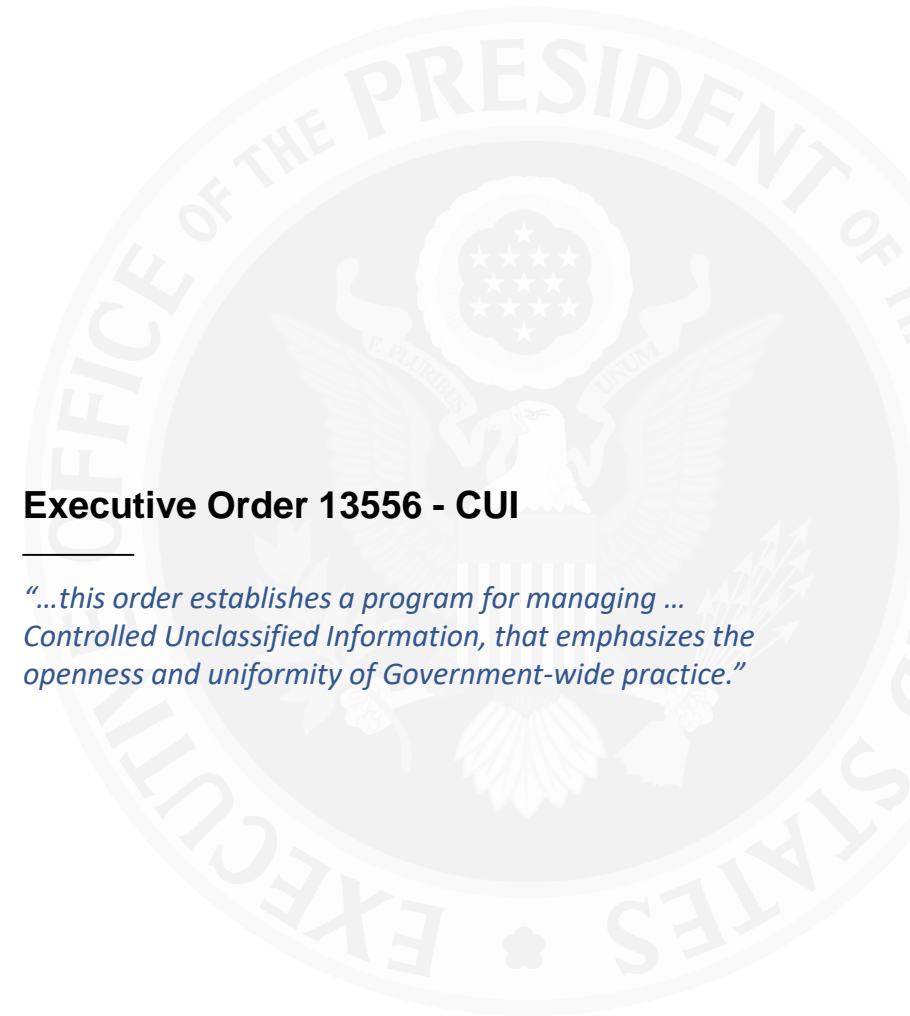
## August 2009

## November 2010



## Executive Order 13556 - CUI

*"...this order establishes a program for managing ... Controlled Unclassified Information, that emphasizes the openness and uniformity of Government-wide practice."*



**October 2016**



**DFARS 252.204-7012 Finalized**

*“Safeguarding Covered Defense Information & Cyber Incident Reporting”*



**FEDERAL REGISTER**

The Daily Journal of the United States Government



**“The CUI Rule” Is Finalized**

*“In written agreements ... that involve CUI, agencies must include provisions that require the entity to handle CUI in accordance with this rule, the Order, and the CUI Registry.”*



**November 2016**

**Special Publication 800-171**

*“Protecting Controlled Unclassified Information in Nonfederal Systems & Organizations.”*

**NIST**

**December 2016**



## “The CUI Rule” Is Finalized

*Part 2002, Title 32, Code of Federal Regulations*



### Subpart A – General Information

- 2002.1 Purpose & Scope
- 2002.2 Incorporation by Reference
- 2002.4 Definitions
- 2002.6 CUI EA
- 2002.8 Roles & Responsibilities

### Subpart B – Key Elements of the CUI Program

- 2002.10 The CUI Registry
- 2002.12 CUI categories
- 2002.14 Safeguarding
- 2002.16 Accessing & Disseminating
- 2002.18 Decontrolling
- 2002.20 Marking
- 2002.22 Limitations
- 2002.24 Agency self-inspection

**November 2016**

### Subpart C – CUI Program Management

- 2002.30 Education & training
- 2002.32 CUI cover sheets
- 2002.34 Transferring records
- 2002.36 Legacy materials
- 2002.38 Waivers
- 2002.44 Disclosure statuses
- 2002.46 Privacy Act
- 2002.48 APA
- 2002.50 Challenges to designation
- 2002.52 Dispute resolution
- 2002.54 Misuse of CUI
- 2002.56 Sanctions for misuse



California's Manufacturing Network

© 2020 CMTC all rights reserved

## “The CUI Rule” Is Finalized

*Part 2002, Title 32, Code of Federal Regulations*



### Subpart A – General Information

- 2002.1 Purpose & Scope
- 2002.2 Incorporation by Reference
- **2002.4 Definitions**
- 2002.6 CUI EA
- 2002.8 Roles & Responsibilities

### Subpart B – Key Elements of the CUI Program

- 2002.10 The CUI Registry
- **2002.12 CUI categories**
- **2002.14 Safeguarding**
- 2002.16 Accessing & Disseminating
- 2002.18 Decontrolling
- 2002.20 Marking
- 2002.22 Limitations
- 2002.24 Agency self-inspection

**November 2016**

### Subpart C – CUI Program Management

- 2002.30 Education & training
- 2002.32 CUI cover sheets
- 2002.34 Transferring records
- 2002.36 Legacy materials
- 2002.38 Waivers
- 2002.44 Disclosure statues
- 2002.46 Privacy Act
- 2002.48 APA
- 2002.50 Challenges to designation
- 2002.52 Dispute resolution
- 2002.54 Misuse of CUI
- 2002.56 Sanctions for misuse



© 2020 CMTC all rights reserved



## “The CUI Rule” Is Finalized

Part 2002, Title 32, Code of Federal Regulations



**November 2016**

### 2002.4 Definitions

2002.12 CUI categories

2002.14 Safeguarding

*“Controlled Unclassified Information (CUI) is information that the Government creates or possesses, or that an entity creates or possesses on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.”*

---

# “The CUI Rule” Is Finalized

*Part 2002, Title 32, Code of Federal Regulations*



# November 2016

## 2002.4 Definitions

## 2002.12 CUI categories

- Critical Infrastructure
- Defense
- Export Control
- Financial
- Immigration
- Intelligence
- International Agreements
- Law Enforcement
- Legal
- Natural & Cultural Resources
- NATO
- Nuclear
- Patent
- Privacy
- Procurement & Acquisition
- Provisional
- Statistical
- Tax
- Transportation

## 2002.14 Safeguarding



California's Manufacturing Network

© 2020 CMTC all rights reserved



## 2002.4 Definitions

## 2002.12 CUI categories

## 2002.14 Safeguarding

- **Defense**
  - Controlled Technical Information (CTI)

“Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.”

---

- Research & Engineering Data
- Engineering Drawings
  - Associated:
    - Specifications
    - Standards
    - Process Sheets
    - Manuals
    - Software & Source Code

## “The CUI Rule” Is Finalized

*Part 2002, Title 32, Code of Federal Regulations*



# November 2016

2002.4 Definitions

2002.12 CUI categories

**2002.14 Safeguarding**

Authorized holders must take reasonable precautions to guard against unauthorized disclosure of CUI...

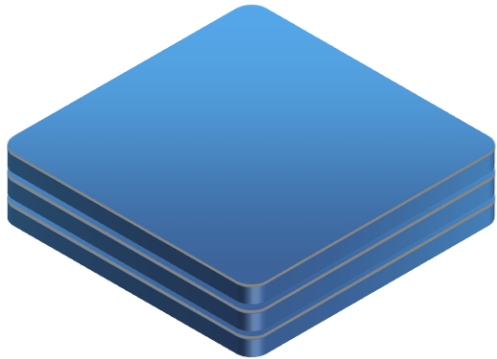
CUI is categorized at no less than moderate confidentiality impact level...

NIST SP 800-171 defines the requirements necessary to protect CUI on non-Federal systems...

**December 2016**

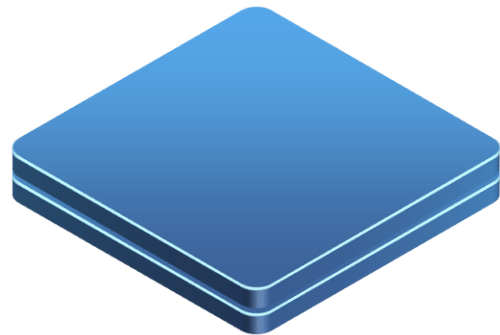
**NIST**

**Special Publication 800-171**





- Confidentiality: unauthorized disclosure
- Moderate Impact: serious adverse effects

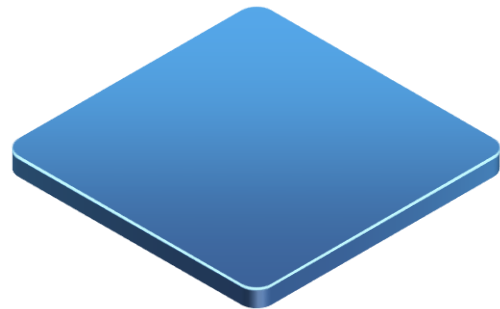


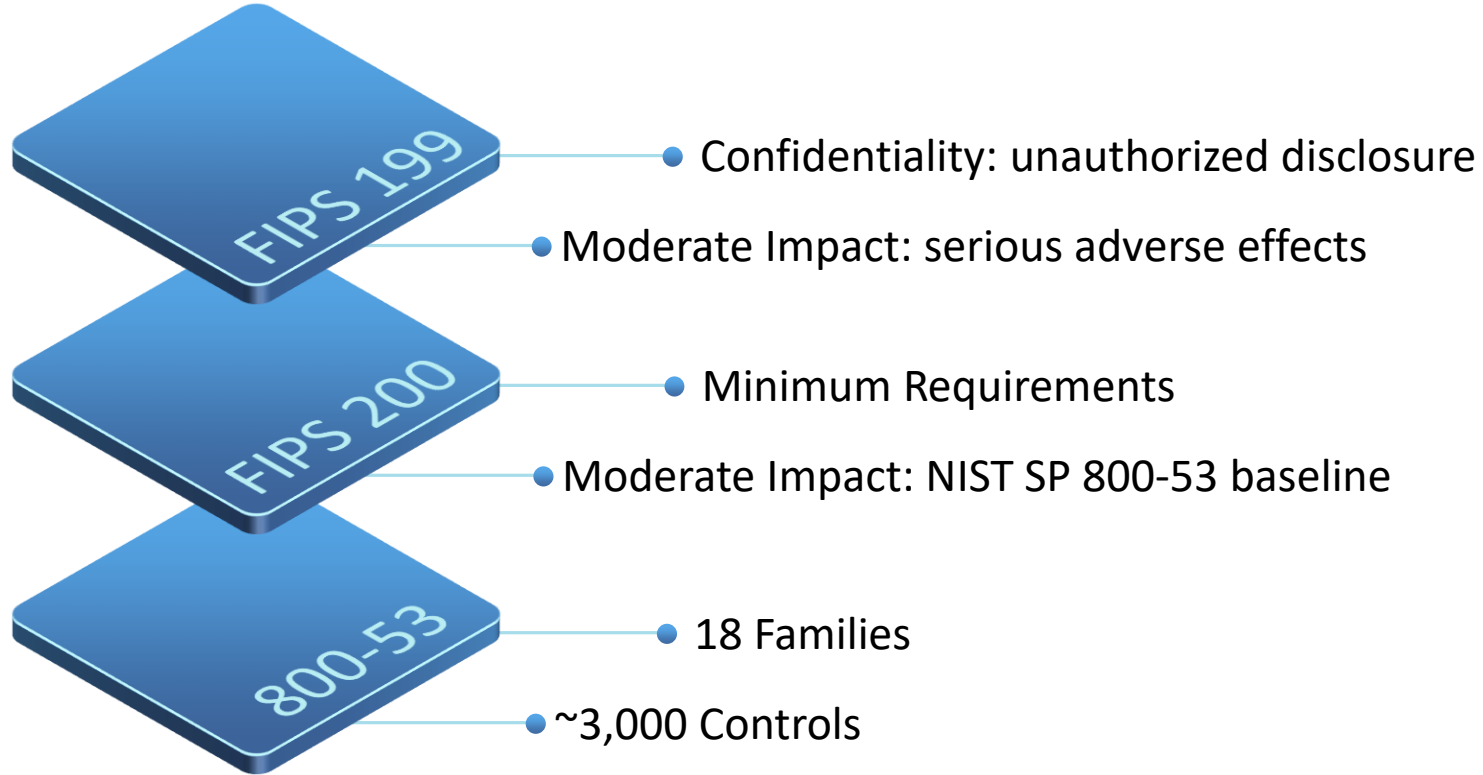


- Confidentiality: unauthorized disclosure
- Moderate Impact: serious adverse effects

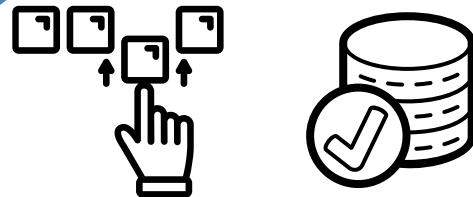
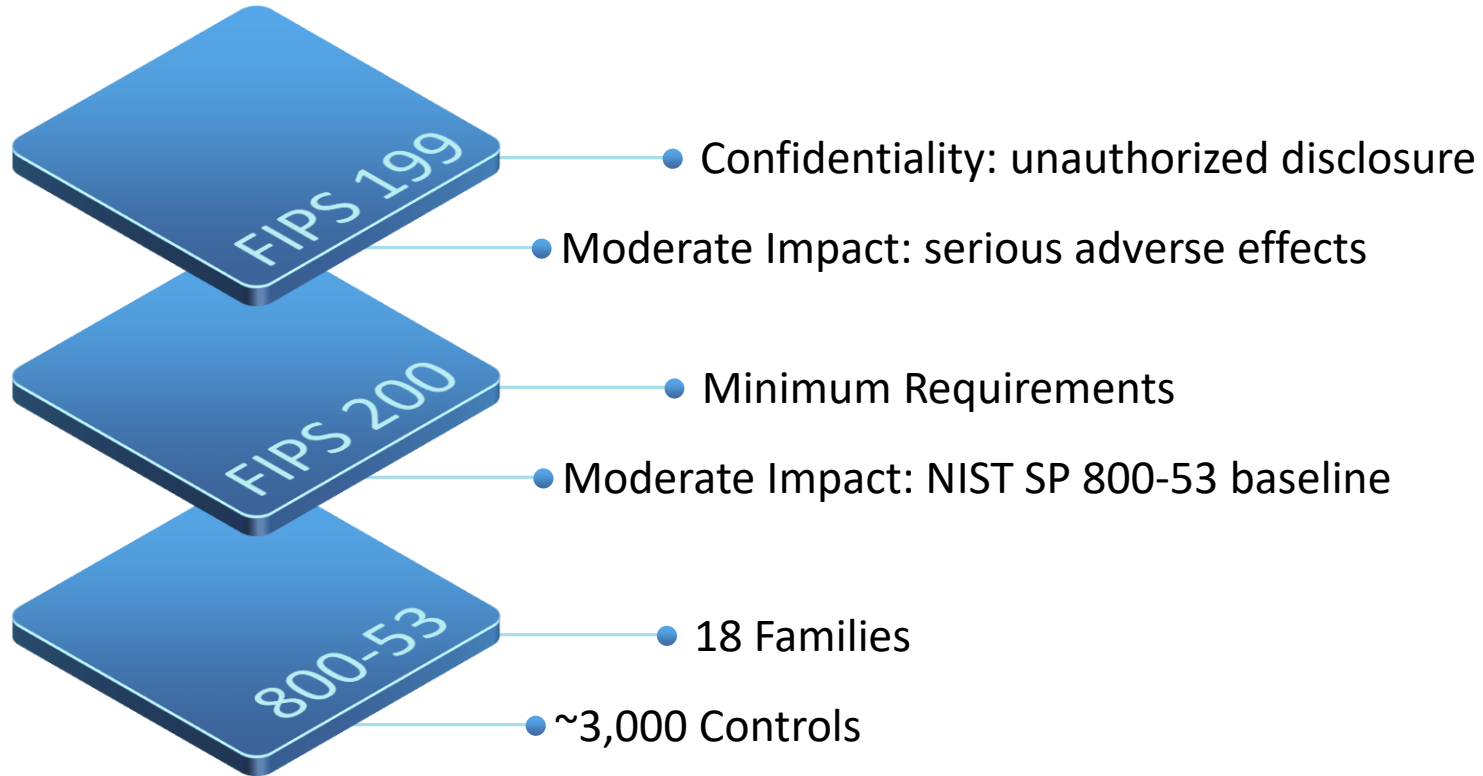


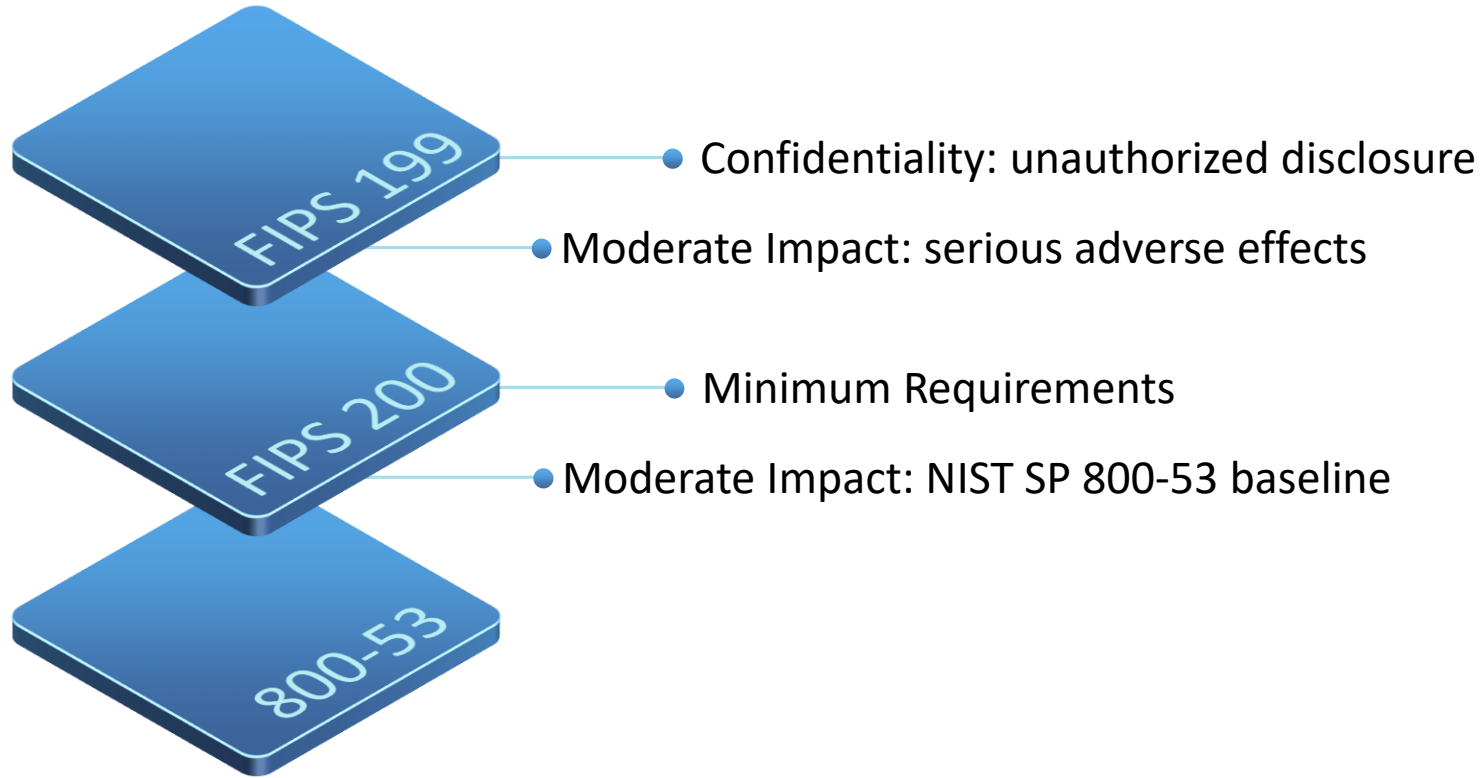
- Minimum Requirements
- Moderate Impact: NIST SP 800-53 baseline

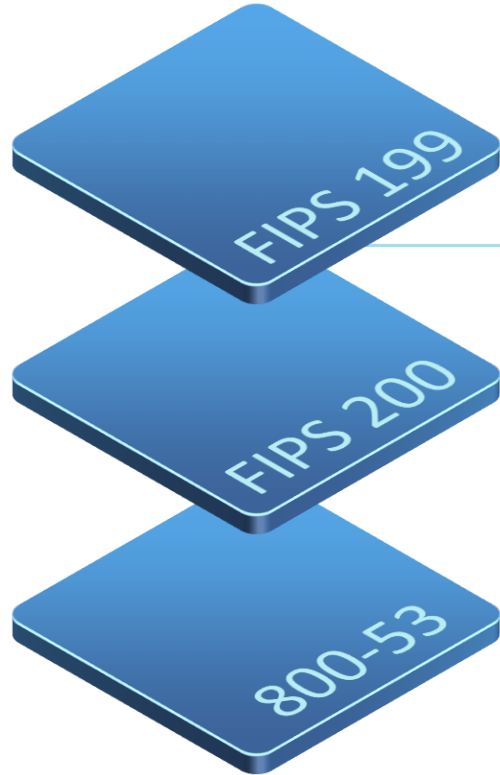




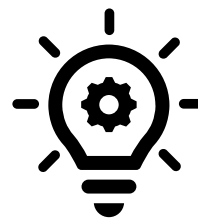








- Confidentiality: unauthorized disclosure
- Moderate Impact: serious adverse effects



NIST Special Publication 800-171  
Revision 2

---

## Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

---

RON ROSS  
VICTORIA PILLITTERI  
KELLEY DEMPSEY  
MARK RIDDLE  
GARY GUISSANIE

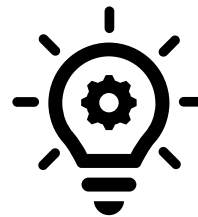
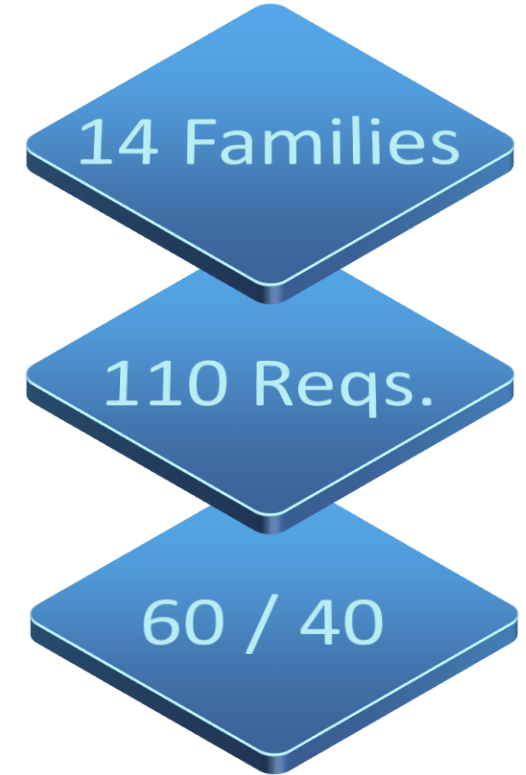
This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.SP.800-171r2>

---

COMPUTER SECURITY

---

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



**CMTC**<sup>®</sup>

California's Manufacturing Network

© 2020 CMTC all rights reserved

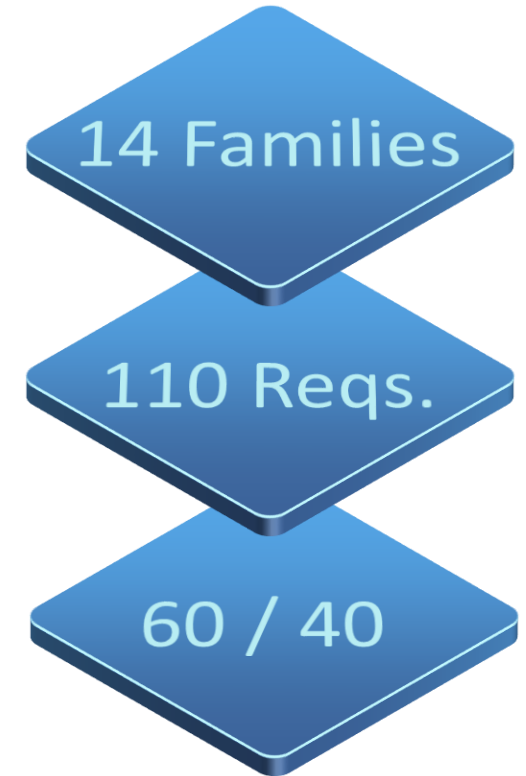


## 63 “NFO” Controls

“Expected to be routinely satisfied by nonfederal organizations without specification.”

SA – System & Services Acquisition

9 – External System Services



### APPENDIX E

#### TAILORING CRITERIA

##### LISTING OF MODERATE SECURITY CONTROL BASELINE AND TAILORING ACTIONS

This appendix provides a list of the security controls in the [SP 800-53]<sup>36</sup> moderate baseline, one of the sources along with [FIPS 200], used to develop the CUI security requirements described in Chapter Three. Tables E-1 through E-17 contain the specific tailoring actions that have been carried out on the controls in accordance with the tailoring criteria established by NIST and NARA. The tailoring actions facilitated the development of the CUI derived security requirements which supplement the basic security requirements.<sup>37</sup> There are three primary criteria for eliminating a security control or control enhancement from the moderate baseline including—

- The control or control enhancement is uniquely federal (i.e., primarily the responsibility of the federal government);
- The control or control enhancement is not directly related to protecting the confidentiality of CUI;<sup>38</sup> or
- The control or control enhancement is expected to be routinely satisfied by nonfederal organizations without specification.<sup>39</sup>

The following symbols in Table E are used in Tables E-1 through E-17 to specify the tailoring actions taken or when no tailoring actions were required.

TABLE E: TAILORING ACTION SYMBOLS

TAILORING SYMBOL	TAILORING CRITERIA
NCO	NOT DIRECTLY RELATED TO PROTECTING THE CONFIDENTIALITY OF CUI.
FED	UNIQUELY FEDERAL, PRIMARILY THE RESPONSIBILITY OF THE FEDERAL GOVERNMENT.
NFO	EXPECTED TO BE ROUTINELY SATISFIED BY NONFEDERAL ORGANIZATIONS WITHOUT SPECIFICATION.
CUI	THE CUI BASIC OR DERIVED SECURITY REQUIREMENT IS REFLECTED IN AND IS TRACEABLE TO THE SECURITY CONTROL, CONTROL ENHANCEMENT, OR SPECIFIC ELEMENTS OF THE CONTROL/ENHANCEMENT.

<sup>36</sup> The security controls in Tables E-1 through E-14 are taken from NIST Special Publication 800-53, Revision 4. These tables will be updated upon publication of [SP 800-53] which will provide an update to the moderate security control baseline consistent with NIST Special Publication 800-53, Revision 5. Changes to the moderate baseline will affect future updates to the basic and derived security requirements in Chapter Three.

<sup>37</sup> The same tailoring criteria were applied to the security requirements in [FIPS 200] resulting in the CUI basic security requirements described in Chapter Three.

<sup>38</sup> While the primary purpose of this publication is to define requirements to protect the confidentiality of CUI, there is a close relationship between the security objectives of confidentiality and integrity. Therefore, the security controls in the [SP 800-53] moderate baseline that support protection against unauthorized disclosure also support protection against unauthorized modification.

<sup>39</sup> The security controls tailored out of the moderate baseline (i.e., controls specifically marked as either NCO or NFO and highlighted in the darker blue shading in Tables E-1 through E-17), are often included as part of an organization's comprehensive security program.



## 63 “NFO” Controls

“Expected to be routinely satisfied by nonfederal organizations without specification.”

---

Requires external service providers comply with organizational information security standards.

Monitors security control compliance by external providers on an ongoing basis.

SLAs define expectations of performance for security controls and identify remedies for noncompliance.

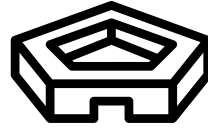
# October 2016



**Final DFARS 252.204-7012 Update**

*Part 252, Title 48, Code of Federal Regulations*

# October 2016



Final DFARS 252.204-7012 Update

*Part 252, Title 48, Code of Federal Regulations*

- a)
- b)
- c)
- d)
- e)
- f)
- g)
- h)
- i)
- j)
- k)
- l)
- m)



**October 2016**



**Final DFARS 252.204-7012 Update**

*Part 252, Title 48, Code of Federal Regulations*

b)

c)

d)

e)

f)

g)

m)

October 2016



Final DFARS 252.204-7012 Update

Part 252, Title 48, Code of Federal Regulations

b)

c)

d)

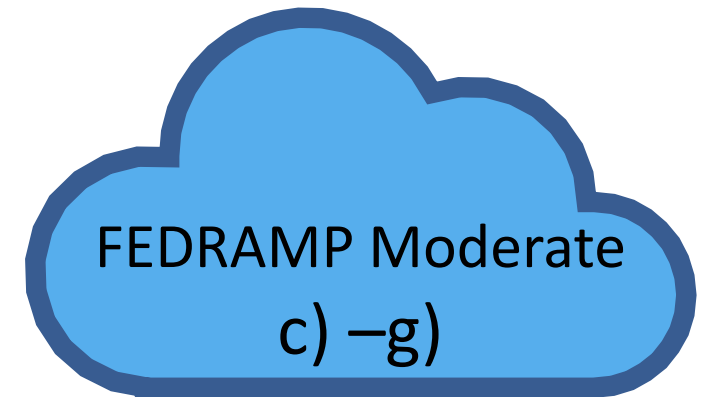
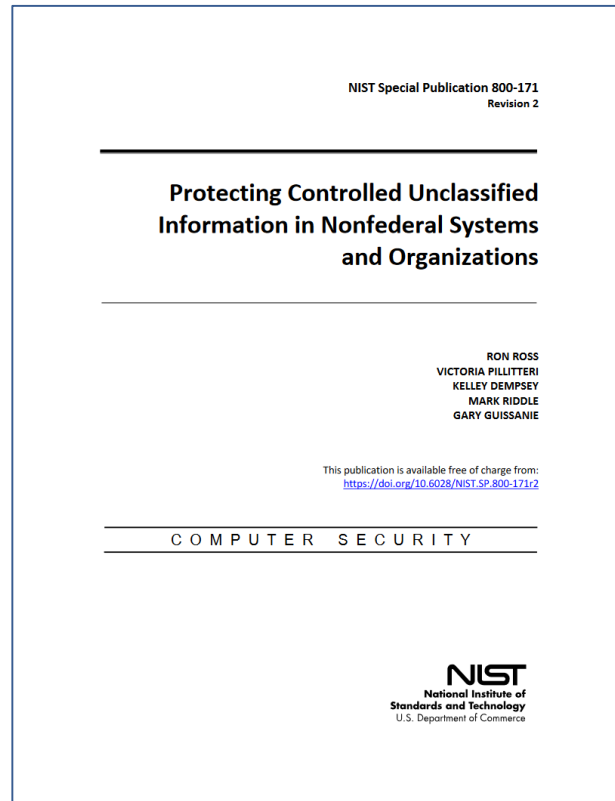
e)

f)

g)

m)

*“Adequate Security”*



October 2016



Final DFARS 252.204-7012 Update

Part 252, Title 48, Code of Federal Regulations

b)

c)

d)

e)

f)

g)

m)

Welcome to the DIBNet portal  
DoD's gateway for defense contractor reporting and voluntary participation in DoD's DIB Cybersecurity Program.

**"Cyber Incident Reporting Requirement"**

**"Rapidly report" = 72 hours**

Report a Cyber Incident

A Medium Assurance Certificate is required to report a Cyber Incident. Applying to the DIB CS Program is not a prerequisite to reporting a Cyber Incident.

DFARS 252.204-7012 Reporting of Cyber Incidents and Cyber Incident Reporting  
DFARS 252.239-7010 Cloud Computing Services

FAR 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities  
FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

Need Assistance?  
Contact DoD Cyber Crime Center (DC3)  
DC3E@dc3.mil  
Hotline: (410) 981-0104  
Toll Free: (877) 838-2174

Apply Now!

The DIB CS Program is a voluntary public-private cybersecurity partnership in which DoD and participating companies share information, investigate, and remediate cyber incidents.

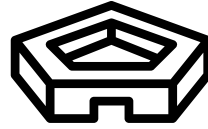
DIB CS Participant Login | Voluntary Report

Trouble Accessing the Site?  
Users with the FPKI Certificate chain are advised to run the **FBCA Certificate Removal Tool** to address chaining issues. **Download** this guide to obtain complete instructions for certificate removal.

Need Assistance?  
Contact the DIB CS Program Office  
OSD.DIBCSIA@mail.mil  
Hotline: (703) 604-3167  
Toll Free: (855) DoD-IACS  
Fax: (571) 372-5434

A DoD-approved Medium Assurance Certificate is required to access DIBNet services. To obtain a DoD-approved Medium Assurance Certificate, please [click here](#).

**October 2016**



**Final DFARS 252.204-7012 Update**

*Part 252, Title 48, Code of Federal Regulations*

b)

c)

**d)**

e)

f)

g)

m)

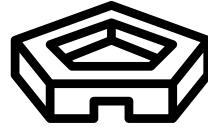
*“Malicious Software”*  
*Submit malware to DC3*



California's Manufacturing Network

© 2020 CMT all rights reserved

**October 2016**



**Final DFARS 252.204-7012 Update**

*Part 252, Title 48, Code of Federal Regulations*

b)

c)

d)

**e)**

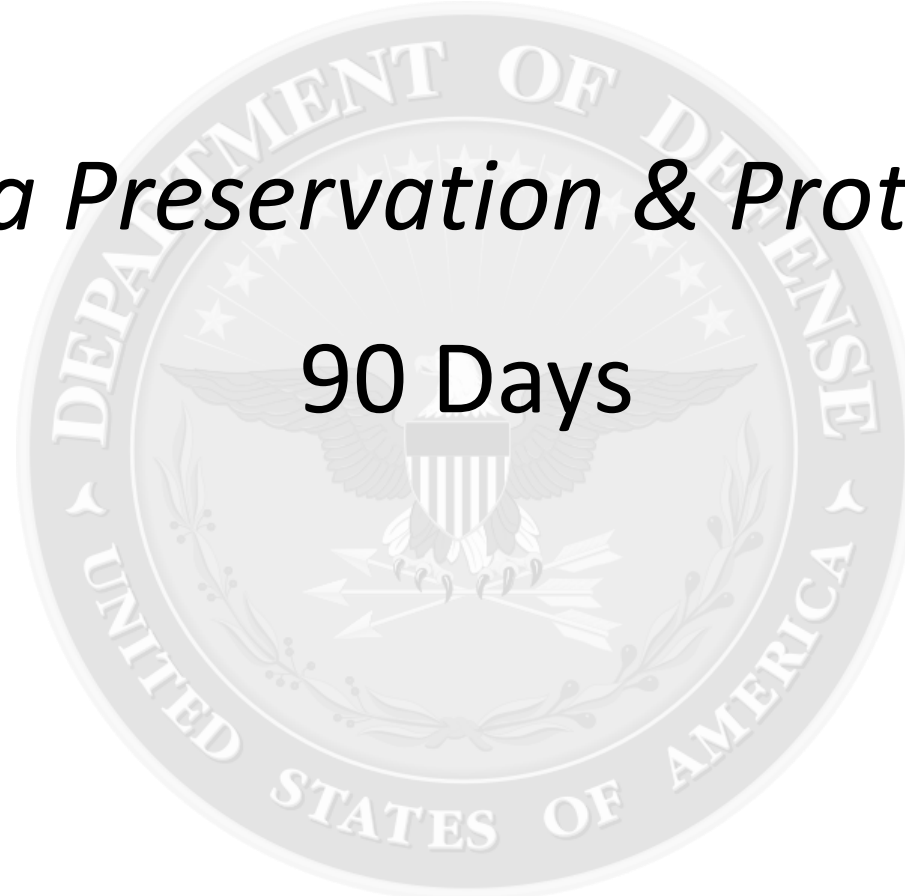
f)

g)

m)

*“Media Preservation & Protection”*

90 Days



**October 2016**



**Final DFARS 252.204-7012 Update**

*Part 252, Title 48, Code of Federal Regulations*

b)

c)

d)

e)

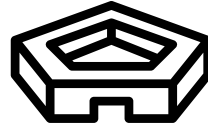
**f)**

g)

m)

*“Access to additional information or equipment necessary for forensic analysis”*

**October 2016**



**Final DFARS 252.204-7012 Update**

*Part 252, Title 48, Code of Federal Regulations*

b)

c)

d)

e)

f)

**g)**

m)

*“Cyber Damage Assessment Activities”*

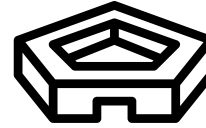
*Provide everything from e)*



California's Manufacturing Network

© 2020 CMTC all rights reserved

# October 2016



Final DFARS 252.204-7012 Update

Part 252, Title 48, Code of Federal Regulations

b)

c)

d)

e)

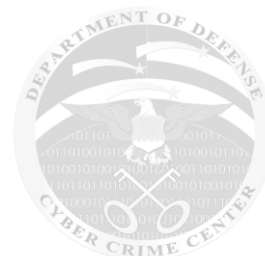
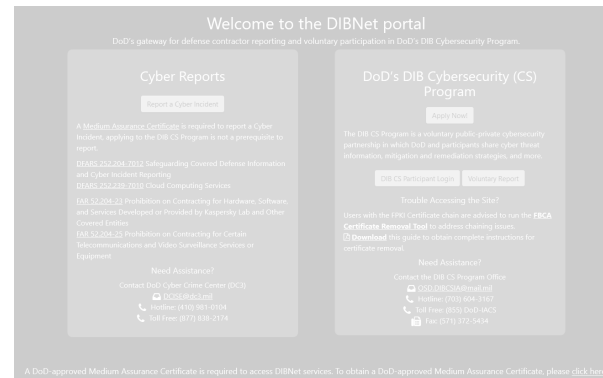
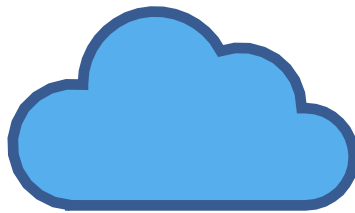
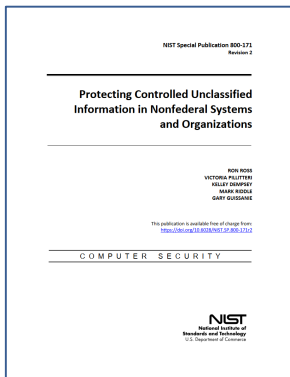
f)

g)

m)

## Safeguarding Covered Defense Information

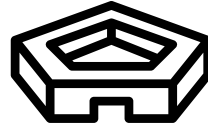
## Cyber Incident Reporting



© 2020 CMTC all rights reserved



**October 2016**



**Final DFARS 252.204-7012 Update**

*Part 252, Title 48, Code of Federal Regulations*

b)

c)

d)

e)

f)

g)

m)

*“Subcontracts”*

**October 2016**



**Final DFARS 252.204-7012 Update**

*Part 252, Title 48, Code of Federal Regulations*

b)

c)

d)

e)

f)

g)



## ***“Subcontracts”***

***“The Contractor Shall –”***

***“Include this clause, including paragraph (m), in subcontracts ...”***

***“For operationally critical support, or for which subcontract performance will include Covered Defense Information...”***

b)

c)

d)

e)

f)

g)

m)



## *“Subcontracts”*

*“The Contractor Shall –”*

*“Include this clause, including paragraph (m), in subcontracts ...”*


*“For operationally critical support, or for which subcontract performance will include Covered Defense Information...”*

---

Requires external service providers  
comply with organizational  
information security standards.

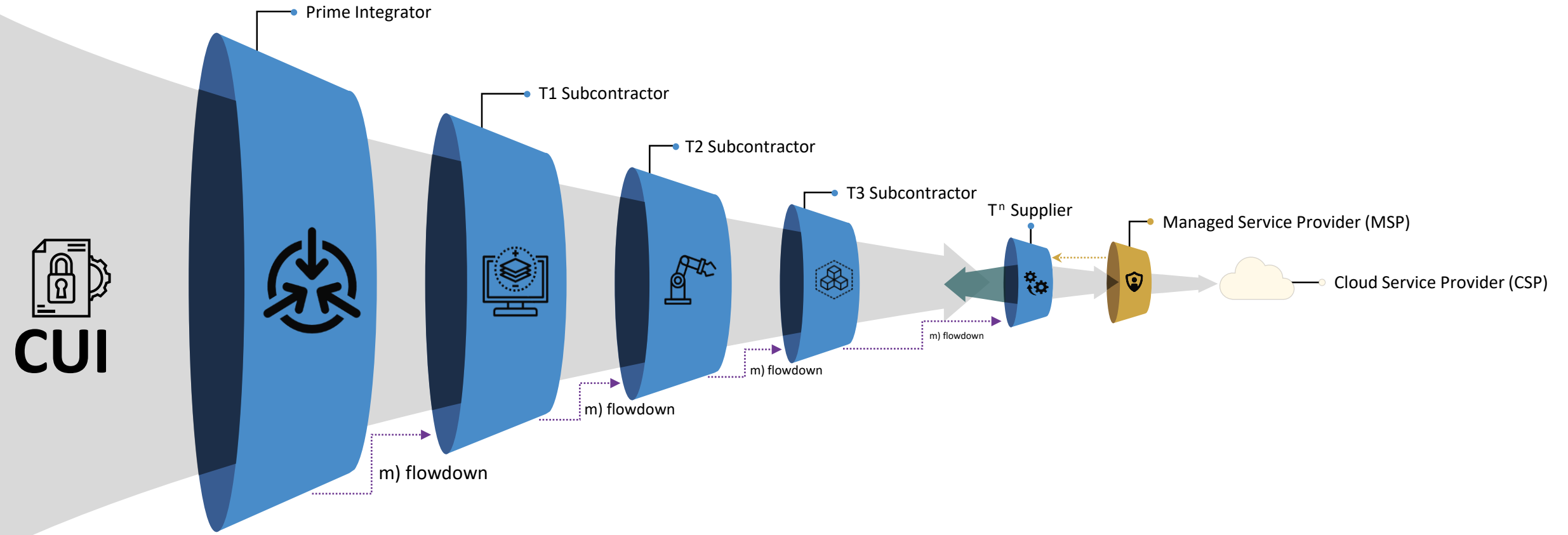
Monitors security control  
compliance by external providers  
on an ongoing basis.

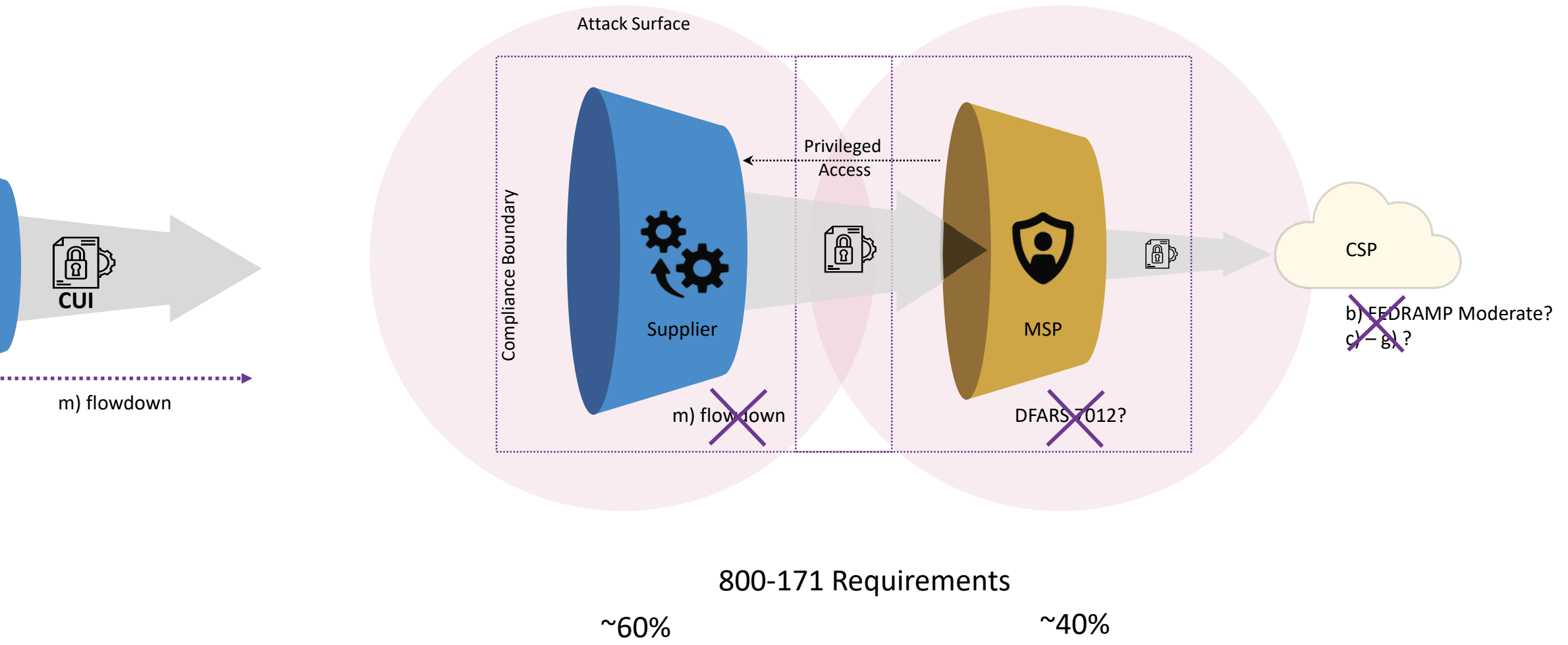
SLAs define expectations of  
performance for security controls and  
identify remedies for noncompliance.





# The Last Mile







# Cybersecurity Maturity Model Certification

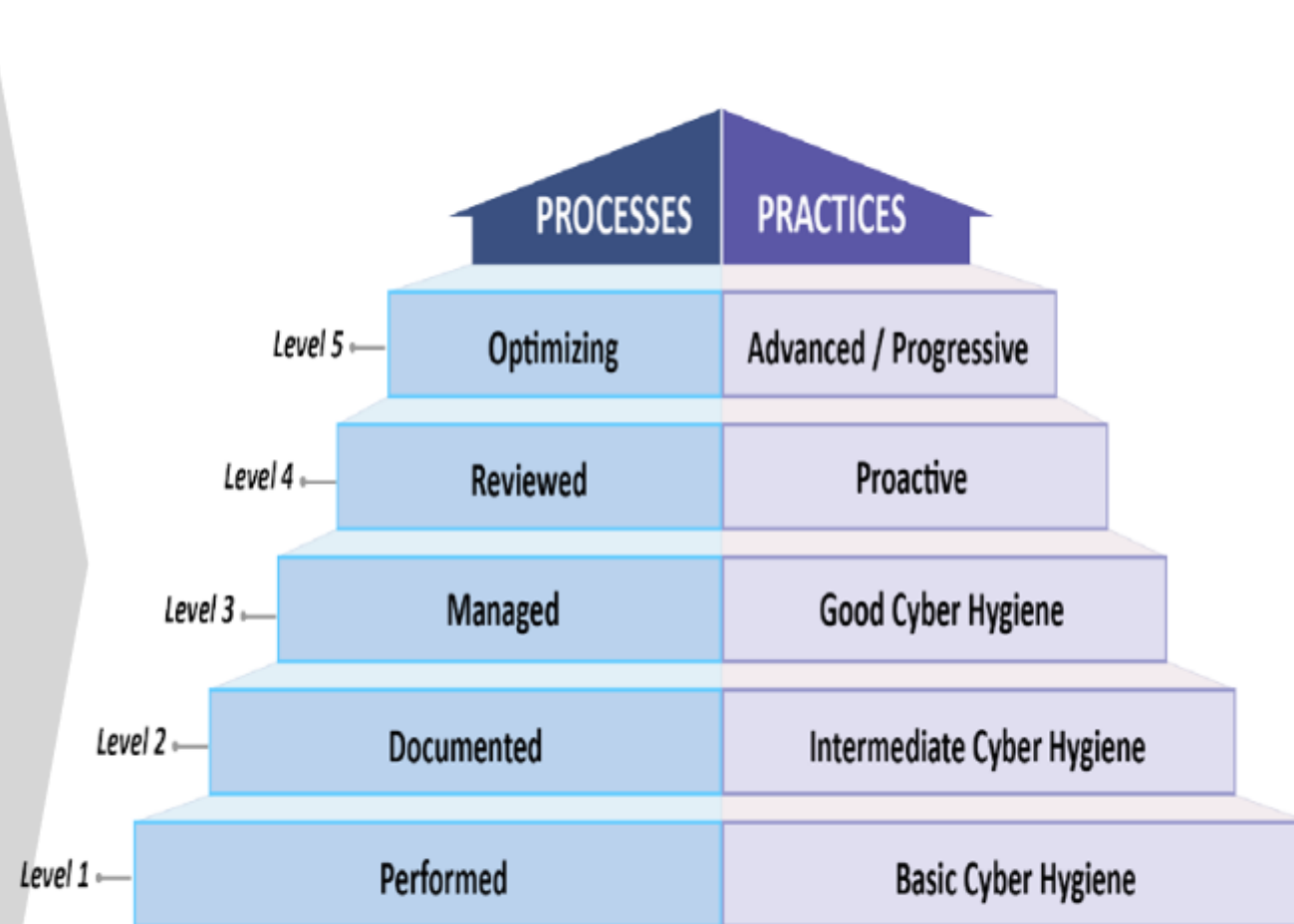
HOW STANDARDS PROLIFERATE:  
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)



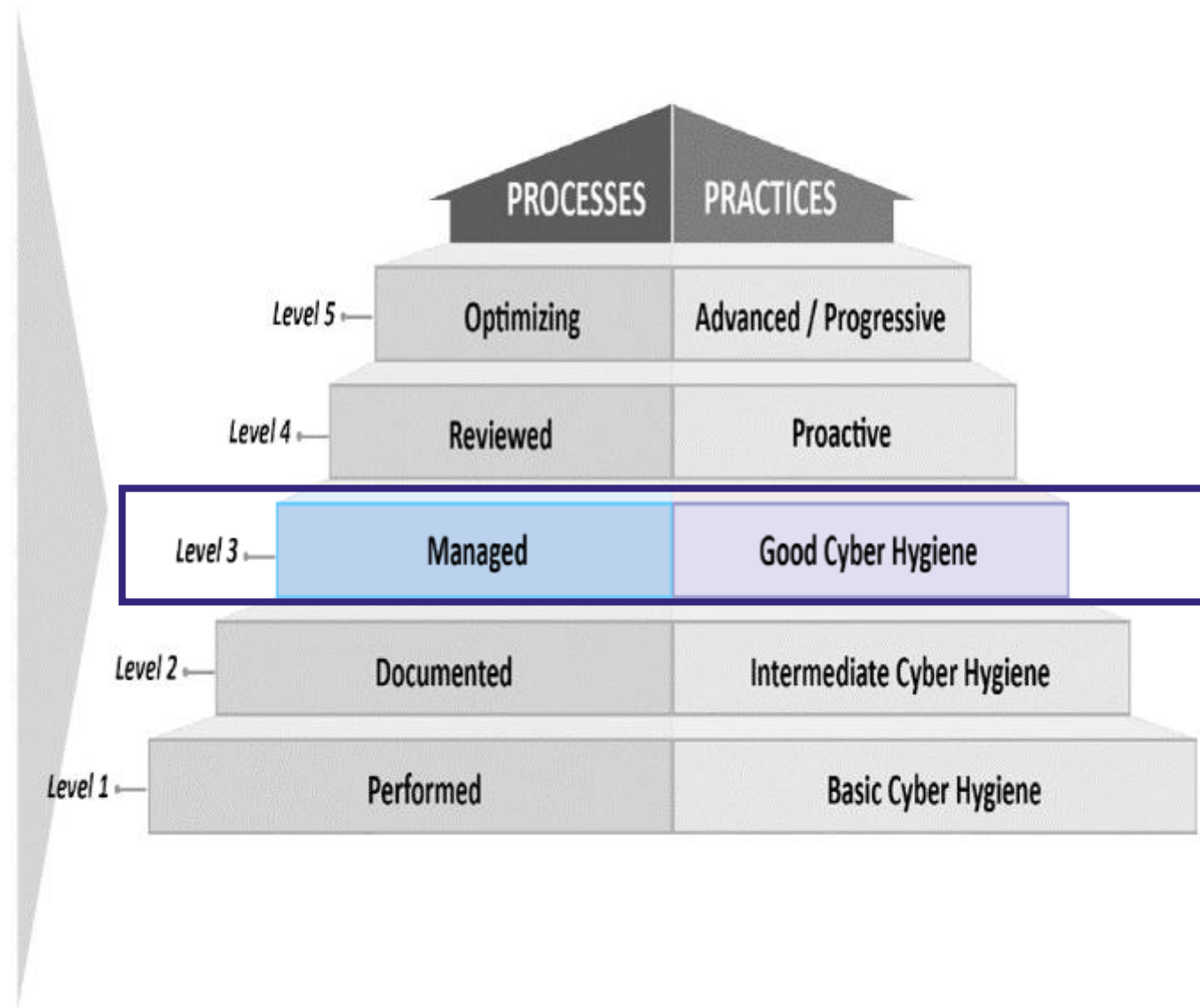
## Cybersecurity Maturity Model Certification

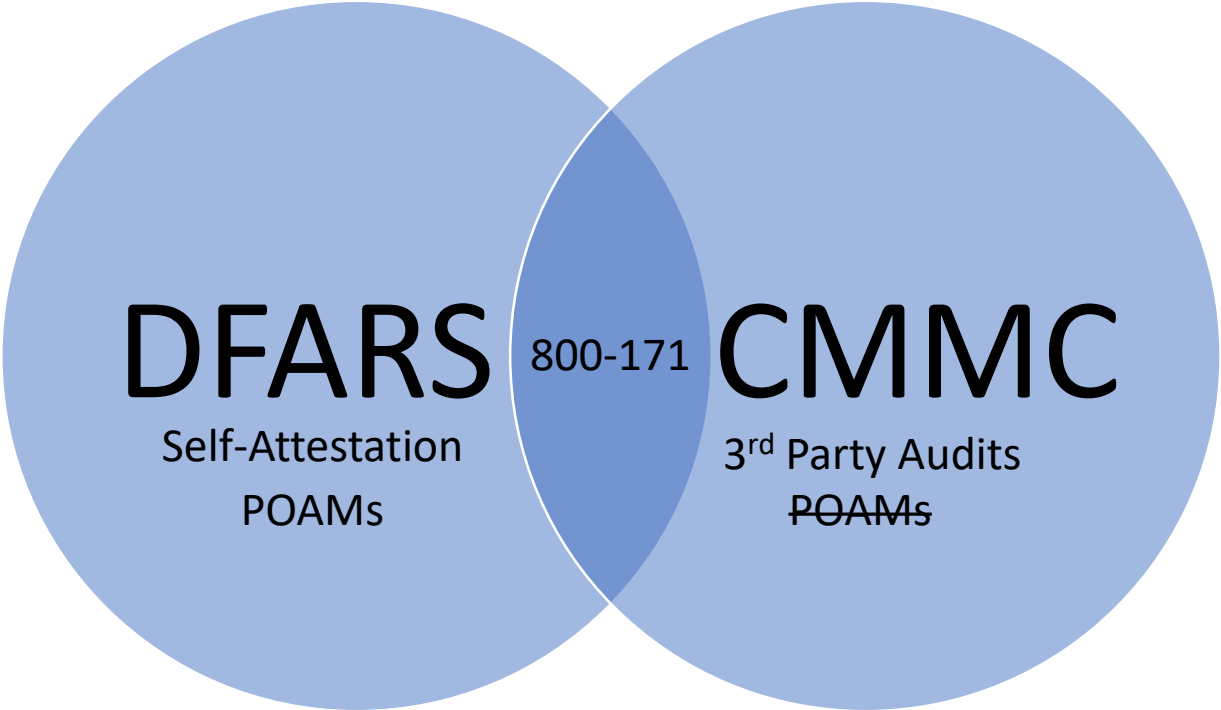


# CMMC Model with 5 levels measures cybersecurity maturity



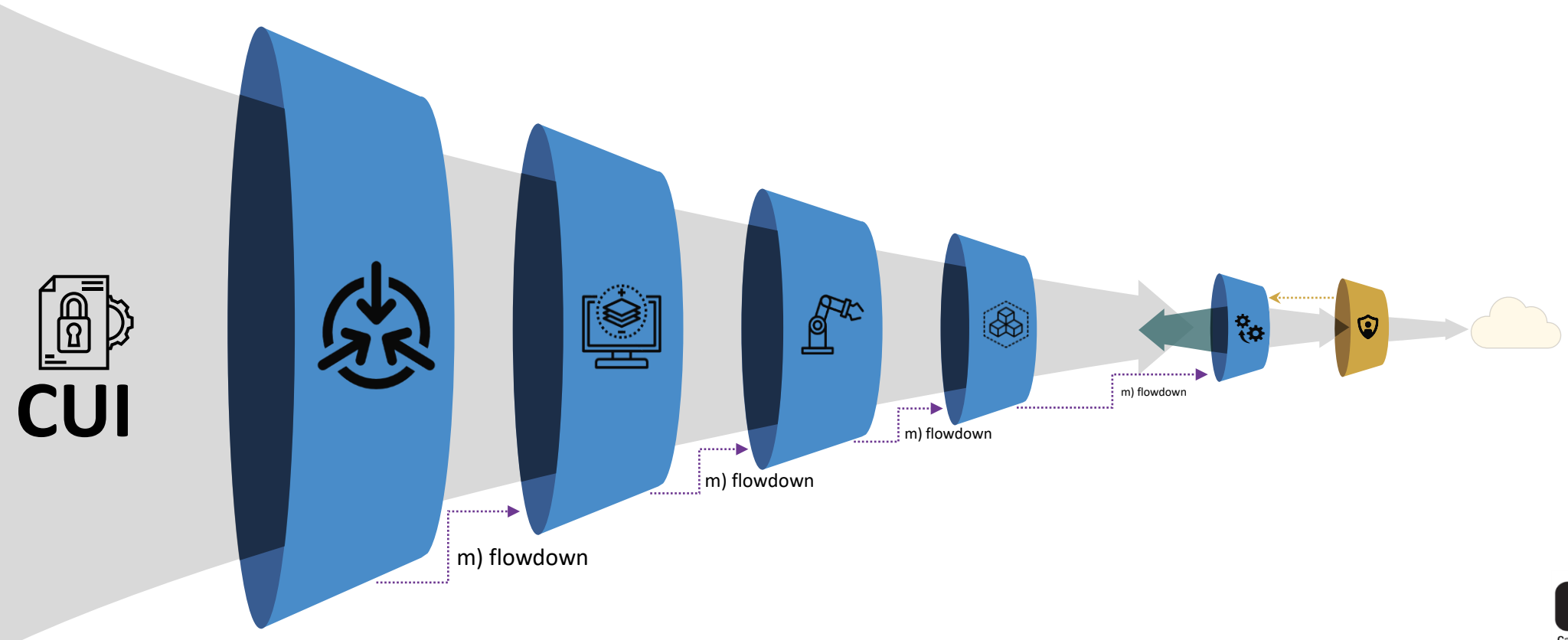
# CMMC Model with 5 levels measures cybersecurity maturity





California's Manufacturing Network

© 2020 CMTc all rights reserved



March 17<sup>th</sup>, 2020

---

**Memorandum of Understanding**

---

between

**The Department of Defense,**

**Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))**

and

**Cybersecurity Maturity Model Certification Accreditation Body, Inc. (CMMC-AB)**

**I. Purpose:**

This Memorandum of Understanding (MOU) sets forth the understandings held by both the Department of Defense (DoD or Department) and the Cybersecurity Maturity Model Certification Accreditation Body, Inc. (CMMC-AB) regarding Cybersecurity Maturity Model Certification (CMMC) accreditation, certification, approval, training and assessment processes as related to the Defense Supply Chain (DSC). The DoD and CMMC-AB are collectively referred to herein as the "parties".

**II. Acceptance of CMMC Certifications**

CMMC-AB is responsible for and authorized to manage, control, and administer CMMC assessment, certification, training, and accreditation processes with respect to the DSC. DoD intends to utilize the results of the CMMC-AB's accreditation efforts to satisfy future DoD solicitation requirements regarding an entity's CMMC certification status.

The Department of Defense will accept only CMMC certifications issued by an assessor who has been accredited to perform CMMC assessments by an Accreditation Body or a CMMC Third Party Assessment Organization (C3PAO) accredited by that same Accreditation Body. The Accreditation Body must be accepted and recognized by the DoD pursuant to a signed Memorandum of Understanding (MOU) or a DoD contract. Any other CMMC certifications are invalid and will not be acceptable to satisfy future DoD solicitation requirements regarding an entity's CMMC certification status.

**III. Background:**

The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) recognizes that security is foundational to acquisition and should not be diminished in favor of cost, schedule, or performance. Therefore, OUSD(A&S) is committed to working with the defense supply chain (DSC) to enhance the protection of federal contract information and Controlled Unclassified Information (CUI) within the DSC. To further this effort, OUSD(A&S) has worked with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDCs), and industry to develop the CMMC Model.

1



Accreditation Body:

8. Require all outsourced IT and/or MSP support organizations to be equivalent CMMC Level 3 certified by government assessors from the DCMA within two years of the date of this MOU.



## Key Takeaways & Next Steps

# 5 Takeaways

Focus on Current DFARS Requirements

Understand 800-171 Assumptions

Establish Vendor Management Process

Understand Flowdown Requirements

Allowable Costs



## Jacob Horne

Senior Cybersecurity Consultant

[jhorne@cmtc.com](mailto:jhorne@cmtc.com)

<https://www.linkedin.com/in/jacob-horne-cissp/>



California's Manufacturing Network

California Manufacturing Technology Consulting

690 Knox Street, Suite 200

Torrance, CA 90502

310.263.3060 | [www.cmtc.com](http://www.cmtc.com)