Evolution

- 2020-09 DFARS Case 2019-D041 implements CMMC 1.0
- 2020-11-30 Interim Rule goes into effect. 5-year phase-in
- 2021-03 DoD launches review
- 2021-11 CMMC 2.0 launch

Key Features

Streamlined Model
- Move from 5 to 3 levels
- Align to NIST standards

Reliable Assessments
- allow for more self assessments a level and 2.
- Increase oversight of C3PAO

Flexible Implementation
- Limited POAM
- Limited Waivers

CMMC 2.0

Tiered Model

Verifiable Assessments

Required in Contracts

CMMC 2.0 implemented through rulemaking

- Part 32 of the Code of Federal Regulations (C.F.R.)
- Defense Federal Acquisition Regulation Supplement (DFARS) Part 48 of C.F.R.

Rule making has public comment period.
DOD will seek stakerholder input, provide training, and incentivize.

Level One

17 Practices
59 Objectives

Annual Self Assessment

Level Two

110 Practices
320 Objectives
NIST-SP-800-171
Annual Self Assessment
or Triannual C3PAO

Level Three

110+ Practices
320+ Objectives
Additional Controls
NIST-SP-800-172
Triannual Governmnet Assessment

Consequence of Non-Compliance

Failure to receive award

Contractual liability

False Clams Act

CYBERDI

ABCs of DFARS 7012

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.

DEFINITIONS

Important Definitions such as controlled technical information and covered defense information.
Defines types of CUI that often fall in scope

ADEQUATE SECURITY

Defines minimum security a contractor must meet by applying requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" and additional requirements around use of cloud vendors, data sovereignty, and approved equipment

Sets a Deadline of December 31, 2017

CYBER INCIDENT REPORTING REQUIREMENT

- Defines legal requirements to report cyber incidents with CDI
- Requires an incident review and response
- Rapid report to DoD
- Medium assurance certificate requirement for reporting but a phone number is avalilable for contractors without a medium assurance certificafe

CYBERDI

DFARS INTERIM CLAUSES

Summary level scores of a current NIST SP 800-171a DoD Assessment Methodology

Basic	Medium | High	CMMC
7019	7020	7021
A contractor with a 7012 clause must condiuct a self-assessment and score thier systems on NIST-SP-800-171 Scores get uploaded to Supplier Performance Risk System (SPRS)	Establishes the Basic, Medium, and High. A Basic uploads summary score (-203-110). A Medium assessment gets reviewed by DoD. A High includes a DoD visit and additional controls and evidence	Cybersecurity Maturity Model Certification as a fraemwork. Requires certification every three years. Only the Undersecretary of A&S can assign the 7021 to contract.

DOD ASSESSMENT METHODOLOGY

Three Methods

Interview

Individuals with responsibilities for specific controls or areas under assessment can get interviewed as evidence

Examine

The majority of evidence will come from document based artifacts with specifications in specific policies and procedures

Test

Often autmomation or employees can get testesd to ensure the policies and procedures happen

SPRS SCORE

To calculate a score to upload you rate yourself against 320 assessment objectives from 171a that match the determination statements of 171. Starting at 110 you subtract either 5, 3, or 1 based on the importance of the control statement

320

ASSESSMENT OBJECTIVES

3.1 AC 22 Controls 70 AOs	3.2 AT 3 Controls 9 AOs	3.3 AU 9 Controls 29 AOs
3.4 CM 9 Controls 44 AOs	3.5 IA 11 Controls 25 AOs	3.6 IR 3 Controls 14 AOs
3.7 MA 22 Controls 70 AOs	3.8 MP 9 Controls 15 AOs	3.9 PS 2 Controls 4 AOs
3.10 PE 6 Controls 16 AOs	3.11 RA 3 Controls 9 AOs	3.12 CA 4 Controls 14 AOs
3.13 SC 16 Controls 41 AOs	3.14 SI 16 Controls 14 AOs	

Horne, J. (2021) As cited by Armyguy298 (2021). Fuzzy Math: The Gap Between SPRS Scores and CMMC Readiness. A Presentation at CS2. Summit Seven San Diego https://discord.com/channels/579151027169918986/579152016173957122/911370252401639484

Score Breakdown

44	14	52
5 pts	3 pts	1 pts

Find the Interim Clauses in Appendix C

A BRIEF HISTORY OF CMMC

CMMC IS A PROGRAM DESIGNED TO INCREASE TRUST IN THE ASSESSMENT OF SUPPLY CHAIN COMPLIANCE TO THE REQUIREMENTS IN NIST-SP-800-171 TO PROTECT CONTROLLED UNCLASSIFIED INFORMATION

IT ALL BEGINS AND ENDS WITH FISMA

2002

Federal Information Security Management Act (2002)
Requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems

Cybersecurity Research and Development Act (2002)
Paid for and authorized National Institute of Standards and Technology (NIST) to establish programs and standards

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

FIPS 199 (2002)
Establishes three categories for protecting data: low,moderate, and high

Homeland Security Presidential Directive 7 (2002)
identify and prioritize critical infrastructure and to protect them from terrorist attacks

2004

FISMA PROJECT (2003)
Published FIPS 199, FIPS 200, and NIST Special Publications 800-53, 800-59, and 800-6. Then 800-37, 800-39, 800-171, 800-53A. Now the Risk Management Project

FISMA
FEDERAL INFORMATION SECURITY MANAGEMENT ACT

2006

2008

National Defense Authorization Act Draft (2008)
First mention of supply chain risk management in the federal congressional record

Executive Order 13556 -Controlled Unclassified Information (2010)
Creates a method to streamline and label sensitive unclassified information after 9/11

2010

National Defense Authorization Act Draft (2010)
NDAA 2011 Contains a section of law dedicated to supply chain risk reduction

CONTROLLED UNCLASSIFIED INFORMATION

Proposed Defense Federal Acquisition Regulations Supplemental rule (2011)
DFARS Case 2011-D039 Requirements for safeguarding unclassified information specifically as it related to fundamental research. Proposed DFARS rule 7000

2012

Proposed Defense Federal Acquisition Regulations Supplemental rule revised (2013)
Updated the proposed clause as it applied to protecting Fundamental research 7000

DFARS 252.204-7000 Rule goes into effect (2013)
Requires the protection of sensitive data on non federal systems

Federal Information Security Modernization Act (2014) 2014
Leads to the Development of NIST Risk Management Framework. DoD decides contractors present a risk due to cybersecurity.

Detection and Avoidance of Counterfeit Electronic Parts-Further Implementation (2014)
acquire electronic parts from trusted suppliers

PDFARS Case 2013-D018 Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Service (2015)
cover the safeguarding of covered defense information .7008-7010 added to address cloud computing

2016

DFARS Case 2014-DOO5 becomes a final rule (2016)
Modifications made to DFARS Case 2014-DOO5 becomes a final rule, and modifies DFARS 7007 and 7008.

DFARS 7012 Interim Period Ends (2016) 2018
By signing a contract carrying the clause, a contractor is self attesting to the implementation of DFARS 7012, and by extension the 110 controls of NIST 800-171.

DoD IG issues a classified report on the cyber security at the Missile Defense Agency (2018)
Report is scathing and results in more attention on Cyber defense

Work on CMMC begins (2019)
In December DoD created the Cybersecurity Maturity Model Program

DoD IG issues second report on the the Missile Defense Agency (2019)
official notice that the DoD supply chain is broadly not implementing the requirements of DFAR 7012

CMMC ACCREDITATION BODY
Cybersecurity Maturity Model Certification

2020

-Jan, First Version of CMMC model released
-March CMMC-AB signs MOU with DoD
Sept-DFARS Interim Rules, 7018-7021 released establishing CMMC
Nov-DoD and CMMC-AB Signs no-cost contract

-March 2021 Deputy of Secretary of the Department of Defense directs an internal review.
-Nov 2021 CMMC 2.0 Model Comes out

- Removes any requirement beyond NIST 171 baseline.
- Reduces levels from five to three,
- Allows self-attestation with affirmation for some data
- Allows POAMs on limited practices
- Returns requirements in alignment with 2016 DFARS rule
- Requirements not in effect on contracts until Federal Rule Making process complete.

2022

CYBERDI

CMMC Timeline for Compliance

May 2023 Is Closer than You Think

CYBERDI

	May/June	July/August	Sept/Oct	Nov/Dec	Jan/Feb	March/April	May 2023
Governance	• Inventory Policy • Choose Frameworks • Identify other standards and regs • Create system to track SSP and POAM	• Identity and Access Management Policies • Access Control Policies • Audit and Accountability Policies • Physical Security	• Configuration Management Policies • Incident Response Policies • Media Protection Policies • Maintenance Policies	Gap Analysis SSP POAM	Triage POAM	Triage POAM	Gap Analysis SSP POAM
Security Team	• Form Team • Risk Assessment • Work with HR on onboarding/exit	• Identity and Access Management Procedures • Access Control Procedures • Audit and Accountability Procedures • Design assessment procedures for each AO	• Configuration Management Procedures • Incident Response Procedures • Media Protection Procedures • Maintenance Procedures • Design assessment procedures				
People and Process	• Form Instructional Leadership team • Develop training matrix based on RMF model • HR focus on AUP	• Identify Training Material • Train staff on MFA • Inscope employees do DoD mandatory CUI training • AUP Awareness • Phishing Awareness/Training	• Risk Awareness all employees • Identify all assets authorized for the system • Hire or contract CCP	• Awareness all employees • Train tier 1 assets • train tier 2 and 3 privileged assets	• Awareness all employees • train tier 2 and an on-privileged assets	• Retrain privileged security users	Review Awareness and Training Proram

Technical Systems	• Identify your tech provider
	  ◦ in house
	  ◦ MSP
	  ◦ Cloud
	• Develop training matrixl
	• HR focus on AUP
		• Inventory all key security assets
		• Identify all assets authorized for the system
			• Set up incident response tools
			• Patch management
			• Test baselien configuration
				• Network Diagrams
				• Data flow diagrams
				• Establish baselien configuration management
					• Anomoly detection
					• SDLC of all assets
					• Patch management
					• test baseline
						• Anomoly detection
						• SDLC of all assets
						• Patch management
						• test baseline
							• Anomoly detection
							• SDLC of all assets
							• Patch management
							• test baseline

Migrate MSP and/or GCC-High

110 Security Requirements of NIST-SP-800-171

CMMC Framework Assesses 171 against 320 Objectives

Access Control

AC.L1-3.1.1 Authorized Access Control
AC.L1-3.1.2 Transaction & Function Control
AC.L2-3.1.3 Control CUI Flow
AC.L2-3.1.4 Separation of Duties
AC.L2-3.1.5 Least Privilege
AC.L2-3.1.6 Non-Privileged Account Use
AC.L2-3.1.7 Privileged Functions
AC.L2-3.1.8 Unsuccessful Logon Attempts
AC.L2-3.1.9 Privacy & Security Notices
AC.L2-3.1.10 Session Lock
AC.L2-3.1.11 Session Termination
AC.L2-3.1.12 Control Remote Access
AC.L2-3.1.13 Remote Access Confidentiality
AC.L2-3.1.14 Remote Access Routing
AC.L2-3.1.15 Privileged Remote Access
AC.L2-3.1.16 Wireless Access Authorization
AC.L2-3.1.17 Wireless Access Protection
AC.L2-3.1.18 Mobile Device Connection
AC.L2-3.1.19 Encrypt CUI on Mobile
AC.L1-3.1.20 External Connections
AC.L2-3.1.21 Portable Storage Use
AC.L1-3.1.22 Control Public Information

Awareness and Training

AT.L2-3.2.1 Role-Based Risk Awareness
AT.L2-3.2.2 Role-Based Training
AT.L2-3.2.3 Insider Threat Awareness

Audit and Accountability

AU.L2-3.3.1 System Auditing
AU.L2-3.3.2 User Accountability
AU.L2-3.3.3 Event Review
AU.L2-3.3.4 Audit Failure Alerting
AU.L2-3.3.5 Audit Correlation
AU.L2-3.3.6 Reduction & Reporting
AU.L2-3.3.7 Authoritative Time Source
AU.L2-3.3.8 Audit Protection
AU.L2-3.3.9 Audit Management

Configuration Management

CM.L2-3.4.1 System Baselining
CM.L2-3.4.2 Security Configuration Enforcement
CM.L2-3.4.3 System Change Management
CM.L2-3.4.4 Security Impact Analysis
CM.L2-3.4.5 Access Restrictions for Change
CM.L2-3.4.6 Least Functionality
CM.L2-3.4.7 Nonessential Functionality
CM.L2-3.4.8 Application Execution Policy
CM.L2-3.4.9 User-Installed Software

Identification and Authentication

IA.L1-3.5.1 Identification
IA.L1-3.5.2 Authentication
IA.L2-3.5.3 Multifactor Authentication
IA.L2-3.5.4 Replay-Resistant Authentication
IA.L2-3.5.5 Identifier Reuse
IA.L2-3.5.6 Identifier Handling
IA.L2-3.5.7 Password Complexity
IA.L2-3.5.8 Password Reuse
IA.L2-3.5.9 Temporary Passwords
IA.L2-3.5.10 Cryptographically-Protected Passwords
IA.L2-3.5.11 Obscure Feedback

Incident Response

IR.L2-3.6.1 Incident Handling
IR.L2-3.6.2 Incident Reporting
IR.L2-3.6.3 Incident Response Testing

Maintenance

MA.L2-3.7.1 Perform Maintenance
MA.L2-3.7.2 System Maintenance Control
MA.L2-3.7.3 Equipment Sanitization
MA.L2-3.7.4 Media Inspection
MA.L2-3.7.5 Nonlocal Maintenance
MA.L2-3.7.6 Maintenance Personnel

Media Protection

MP.L1-3.8.3 Media Disposal
MP.L2-3.8.1 Media Protection
MP.L2-3.8.2 Media Access
MP.L2-3.8.4 Media Markings
MP.L2-3.8.5 Media Accountability
MP.L2-3.8.6 Portable Storage Encryption
MP.L2-3.8.7 Removeable Media
MP.L2-3.8.8 Shared Media
MP.L2-3.8.9 Protect Backups

Personnel Security

PS.L2-3.9.1 Screen Individuals
PS.L2-3.9.2 Personnel Actions

Physical Protection

PE.L1-3.10.1 Limit Physical Access
PE.L2-3.10.2 Monitor Facility
PE.L1-3.10.3 Escort Visitors
PE.L1-3.10.4 Physical Access Logs
PE.L1-3.10.5 Manage Physical Access
PE.L2-3.10.6 Alternative Work Sites

Risk Assessment

RA.L2-3.11.1 Risk Assessments
RA.L2-3.11.2 Vulnerability Scan
RA.L2-3.11.3 Vulnerability Remediation

Security Assessment

CA.L2-3.12.1 Security Control Assessment
CA.L2-3.12.2 Plan of Action
CA.L2-3.12.3 Security Control Monitoring
CA.L2-3.12.4 System Security Plan

Systems and Communication Protection

SC.L1-3.13.1 Boundary Protection
SC.L2-3.13.2 Security Engineering
SC.L2-3.13.3 Role Separation
SC.L2-3.13.4 Shared Resource Control
SC.L1-3.13.5 Public-Access System Separation
SC.L2-3.13.6 Network Communication by Exception
SC.L2-3.13.7 Split Tunneling
SC.L2-3.13.8 Data in Transit
SC.L2-3.13.9 Connections Termination
SC.L2-3.13.10 Key Management
SC.L2-3.13.11 CUI Encryption
SC.L2-3.13.12 Collaborative Device Control
SC.L2-3.13.13 Mobile Code
SC.L2-3.13.14 Voice over Internet Protocol
SC.L2-3.13.15 Communications Authenticity
SC.L2-3.13.16 Data at Rest

System and Information Integrity

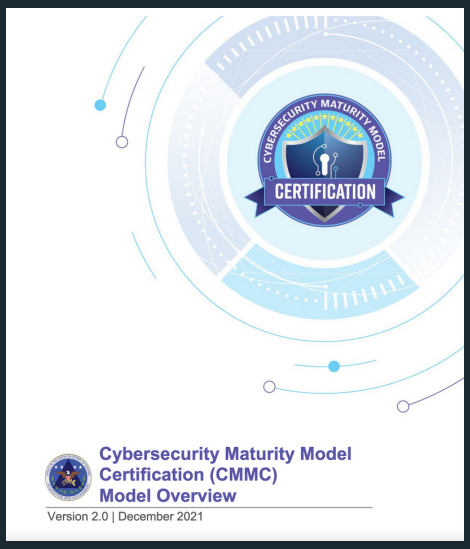
SI.L1-3.14.1 Flaw Remediation
SI.L1-3.14.2 Malicious Code Protection
SI.L2-3.14.3 Security Alerts & Advisories
SI.L1-3.14.4 Update Malicious Code Protection
SI.L1-3.14.5 System & File Scanning
SI.L2-3.14.6 Monitor Communications for Attacks
SI.L2-3.14.7 Identify Unauthorized Use

CYBERDI

CMMC Documents

Model Overview

https://www.acq.osd.mil/cmmc/docs/ModelOverview_V2.0_FINAL2_20211202_508.pdf



- Security requirements from NIST SP 800-171 Rev 2, and a subset of the requirements from NIST SP 800-172
- Organized practices into a set of domains, which map directly to the NIST SP 800-171 Rev 2 families.
- Three Levels
- 14 Domains
- 110 Practices

CYBERDI

Level One Assessment Guide

https://www.acq.osd.mil/cmmc/docs/AG_Level1_V2.0_FinalDraft_20211210_508.pdf

- Provides self-assessment guidance for Level 1
- Contractor must specify the CMMC Self-Assessment Scope
- Leverages the assessment procedure described in NIST Special Publication (SP) 800-171A modified for FCI
- Describes documents, mechanisms, or activities to examine, people to interview, and systems to test

Level Two Assessment Guide

https://www.acq.osd.mil/cmmc/docs/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

https://www.acq.osd.mil/cmmc/docs/Scope_Level1_V2.0_FINAL_20211202_508.pdf

- Provides self-assessment and third party guidance for Level 12
- Contractor and third party assessor must agree to CMMC Scope
- Assessment procedure in NIST-SP-800-171a
- Describes documents, mechanisms, or activities to examine, people to interview, and systems to test
- Separation techniques for out of scope assets
- External Provider Considerations

Level One Scoping Guide

https://www.acq.osd.mil/cmmc/docs/Scope_Level1_V2.0_FINAL_20211202_508.pdf

Federal Contract Information (FCI)

Assets process, store, or transmit FCI a
- Process – FCI can be used by an asset
- Store – FCI is inactive or at rest on an asset
- Transmit – FCI is being transferred from one asset to another asset

FCI is everywhere in systems used for Government contracting. Consider the scope a baseline

Level Two Scoping Guide

https://www.acq.osd.mil/cmmc/docs/Scope_Level2_V2.0_FINAL_20211202_508.pdf

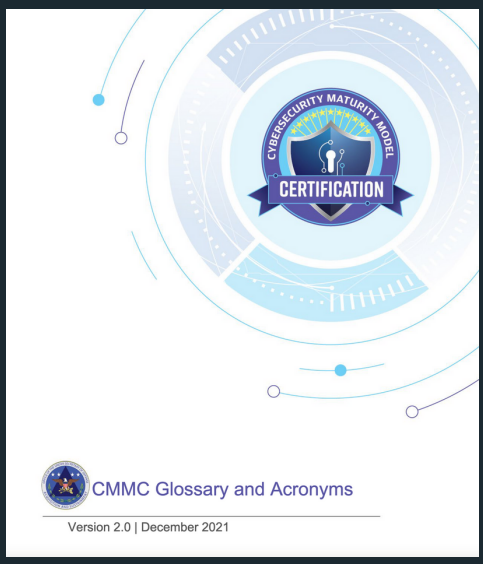
Controlled Unclassified Information

Maps contractor assets into one of five categories:
- CUI assets,
- Security Protection Assets,
- Contractor Risk Managed Assets,
- Specialized assets
- Out of Scop assets

Glossary

https://www.acq.osd.mil/cmmc/docs/Glossary_MasterV2.0_FINAL_202111217_508.pdf

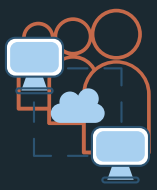
Terms used in CMMC and their sources



Hashing Guide

https://www.acq.osd.mil/cmmc/docs/HashingGuide_V2.0_FINAL_20211203.pdf

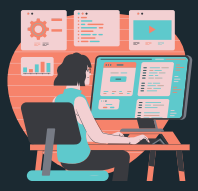
Directions on hashing with PowerShell



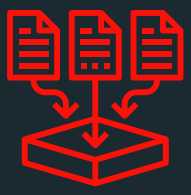
Match Company Architecture

Define System Components

Define Mission and Business Process



Identify IT, Security and Boss People



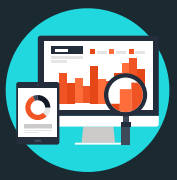
Identify How CUI and FCI Moves

Categorize Assets

SYSTEM SECURITY PLAN

USE THE CUI SSP TEMPLATE FROM NIST

Identify Threats



Assess Risk to Personal Data

Identify Vendors and Cloud Providers

Procedures used to meet CMMC Assessment Objectives

Other frameworks used in risk based plan

Risk Assessment of security procedures

Planning Process to Write and Revlew SSP

CYBERDI

Document History and Approval

Source: 3.12.PL-2 NIST-SP-800-53 as cited in TABLE D-12: MAPPING SECURITY ASSESSMENT REQUIREMENTS TO CONTROLS Appendix E NIST-SP-800-171.

Security Systems Engineering Approach to the SSP

Problem

- Define CMMC Practice
- Identify Assessment Objects
- Identify Assets Protected by the Practice
- Identify Assets that protect the asset
- Collect lifecycle of any asset

Solution

- Identify policy aligned to practice
- Identify baseline deployment for technical asset
- Create/automate procedures to deploy asset to baseline
- Verify asset is deployed correctly

Continuous Improvement through automated asset management and reference architecture

Analyze

- Create feedback loop for continuous improvement
- Review the SSP
- Identify Items in POAM to triage based on risk assessment

Trustworthiness

- Choose assessment method that provides greatest breadth of evidence
- Collect evidence to ensure depth of coverage
- If adequate requirements not met create an item in the POAM

CYBERDI

CYBERDI

FCI VERSUS CUI

COMPARING THE 2 TYPES CONTRACT DATA

Who made it?

FCI can be created by you or the government as a result of contract.

FCI is not intended for public release

Who made it?

CUI can be created by you or the government as a result of a contract.

CUI requires additonal security by law, regulation, or policy

What is it?

any information included in or created for a contract not meant for public release

What is it?

information that needs safeguarding or dissemination protection required by law, regulation, or government wide policy, excluding nuclear and classified information

What Kinds?

There is no labeling system for FCI

All contract information not intended for the public is FCI.

What Kinds?

CUI-Basic
CUI-Specified
CUI-Specified is different. It does not get higher protection.

Specified just identifies additional protections required

Who Labels?

FCI needs safeguarding

There is no requirement to label.

Who Labels?

The person generating, under agency authorization, marks CUI. Anyone who disseminates, or stores must follow markng rules.

CYBERDI

FCI VERSUS CUI

COMPARING THE 2 TYPES CONTRACT DATA

History?

Established by the Federal Aquisition Regulation Cluase 52.204-21 Basic Safeguarding of Covered Contractor Information Systems

History?

Created after 9/11 by Executive Order 13556 to create a streamlined method for data sharing.

Protected?

FAR 52.204-21 lays out 15 basic safeguards for data protection.
17 practices from NIST-800-171

Protected?

CUI gets protected by 110 practices from NIST-800-171

Is my IP FCI?

Your IP can not be FCI

Is My IP CUI?

Usually not, but if your IP falls under CUI, this must get spelled out in the contract

CMMC?

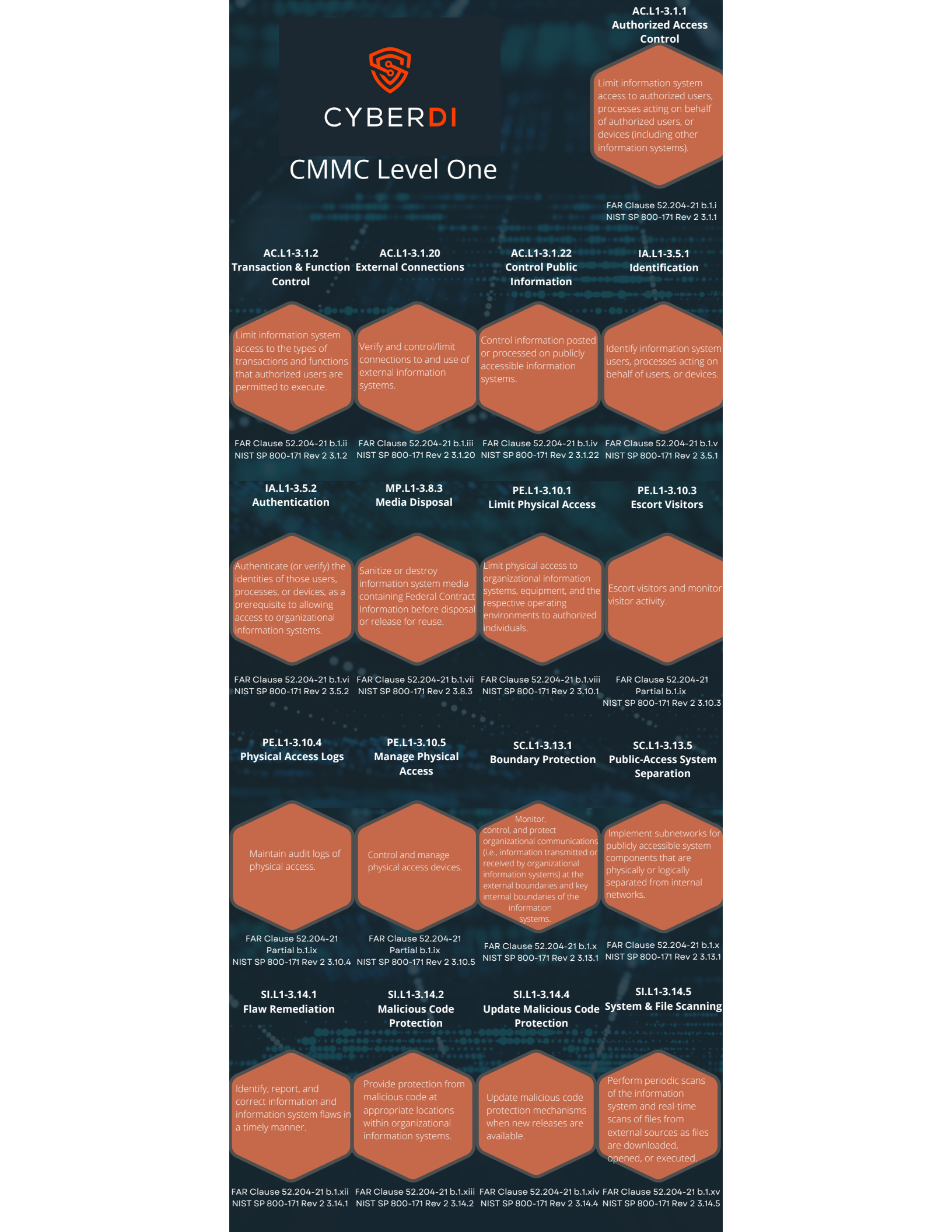
Any contractor who handles FCI must achieve a CMMC Maturity Level 1 which involes a self assessment against the 17 practivces

CMMC?

Any contractor who handles CUI needs a Maturity Level 2

Some Is will require third party assessments

Some Level 3 Contracts will require additional requirements from 172


CYBERDI
CMMC Level One
AC.L1-3.1.1
Authorized Access Control
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 2 3.1.1
AC.L1-3.1.2
Transaction & Function Control
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 2 3.1.2
AC.L1-3.1.20
External Connections
Verify and control/limit connections to and use of external information systems.
FAR Clause 52.204-21 b.1.iii
NIST SP 800-171 Rev 2 3.1.20
AC.L1-3.1.22
Control Public Information
Control information posted or processed on publicly accessible information systems.
FAR Clause 52.204-21 b.1.iv
NIST SP 800-171 Rev 2 3.1.22
IA.L1-3.5.1
Identification
Identify information system users, processes acting on behalf of users, or devices.
FAR Clause 52.204-21 b.1.v
NIST SP 800-171 Rev 2 3.5.1
IA.L1-3.5.2
Authentication
Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
FAR Clause 52.204-21 b.1.vi
NIST SP 800-171 Rev 2 3.5.2
MP.L1-3.8.3
Media Disposal
Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
FAR Clause 52.204-21 b.1.vii
NIST SP 800-171 Rev 2 3.8.3
PE.L1-3.10.1
Limit Physical Access
Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
FAR Clause 52.204-21 b.1.viii
NIST SP 800-171 Rev 2 3.10.1
PE.L1-3.10.3
Escort Visitors
Escort visitors and monitor visitor activity.
FAR Clause 52.204-21 Partial b.1.ix
NIST SP 800-171 Rev 2 3.10.3
PE.L1-3.10.4
Physical Access Logs
Maintain audit logs of physical access.
FAR Clause 52.204-21 Partial b.1.ix
NIST SP 800-171 Rev 2 3.10.4
PE.L1-3.10.5
Manage Physical Access
Control and manage physical access devices.
FAR Clause 52.204-21 Partial b.1.ix
NIST SP 800-171 Rev 2 3.10.5
SC.L1-3.13.1
Boundary Protection
Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
FAR Clause 52.204-21 b.1.x
NIST SP 800-171 Rev 2 3.13.1
SC.L1-3.13.5
Public-Access System Separation
Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
FAR Clause 52.204-21 b.1.x
NIST SP 800-171 Rev 2 3.13.1
SI.L1-3.14.1
Flaw Remediation
Identify, report, and correct information and information system flaws in a timely manner.
FAR Clause 52.204-21 b.1.xii
NIST SP 800-171 Rev 2 3.14.1
SI.L1-3.14.2
Malicious Code Protection
Provide protection from malicious code at appropriate locations within organizational information systems.
FAR Clause 52.204-21 b.1.xiii
NIST SP 800-171 Rev 2 3.14.2
SI.L1-3.14.4
Update Malicious Code Protection
Update malicious code protection mechanisms when new releases are available.
FAR Clause 52.204-21 b.1.xiv
NIST SP 800-171 Rev 2 3.14.4
SI.L1-3.14.5
System & File Scanning
Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
FAR Clause 52.204-21 b.1.xv
NIST SP 800-171 Rev 2 3.14.5

Asset Categorization

Counting, Sorting, and Documenting all assets, both organizational and government owned, to determine scope of an IT system

Technology

Computers, portable storage, mobile devices, endpoints, routers, switches, wires, servers, Cloud, VPN, MFA, MDM,

People

- Anyone with legal need to access CUI or FCI
- Anyone who protects, monitors or access sysetems that protect CUI

Facilities

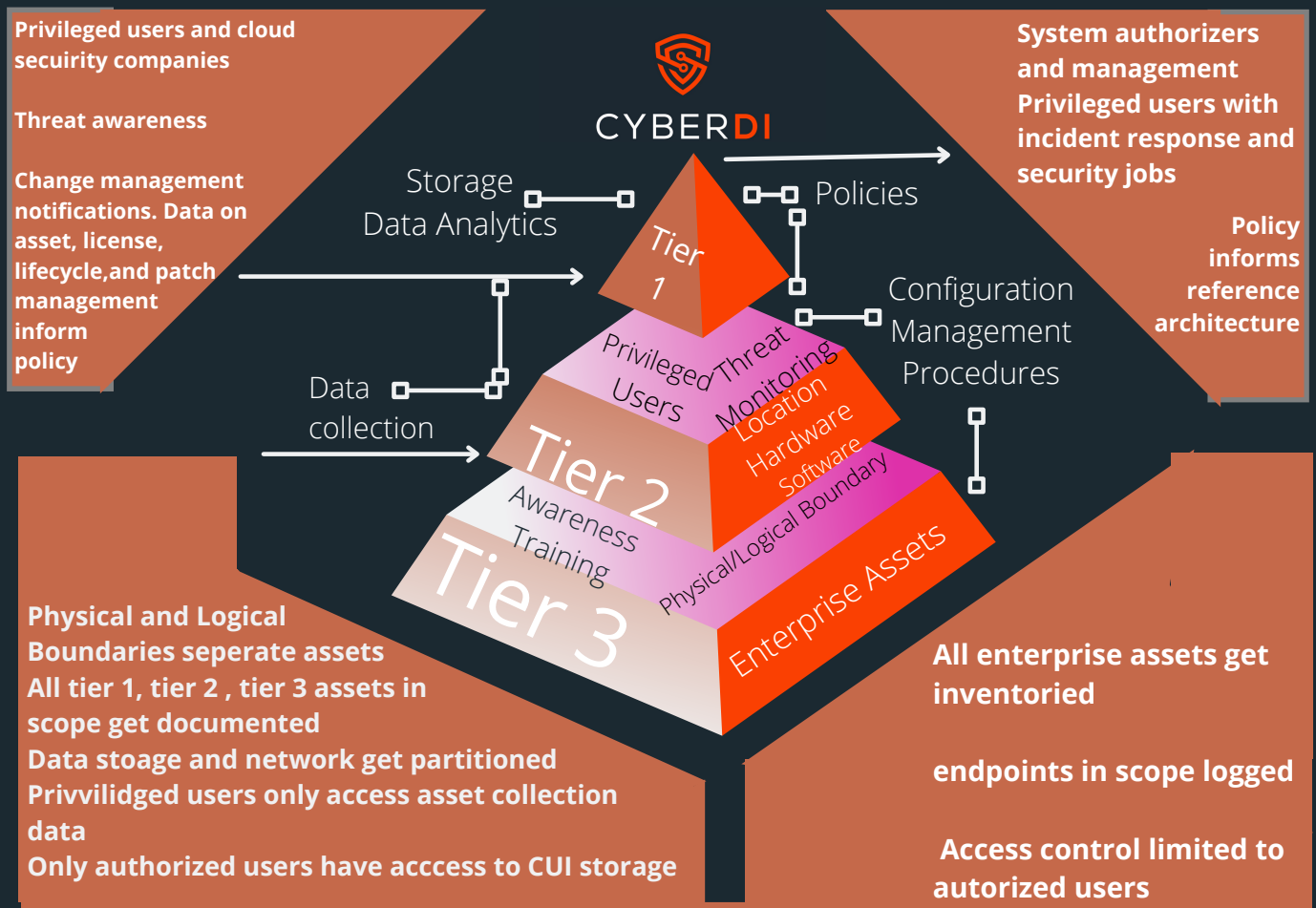
Headquarters, hosting agency, vehicles, co-located data center, remote employee work station,

FOLLOW THE DATA

Privileged users and cloud secuirity companies

Threat awareness

Change management notifications. Data on asset, license, lifecycle,and patch management inform policy



System authorizers and management Privileged users with incident response and security jobs

Policy informs reference architecture

Physical and Logical Boundaries seperate assets
All tier 1, tier 2 , tier 3 assets in scope get documented
Data stoage and network get partitioned
Privvilidged users only access asset collection data
Only authorized users have acccess to CUI storage

All enterprise assets get inventoried

endpoints in scope logged

Access control limited to autorized users

THREE METHODS

Manual

metadatags applied by the user or security personel to the data or file

Automatic

scanning data for CUI marking or analyzing the text or file size and assigning a label

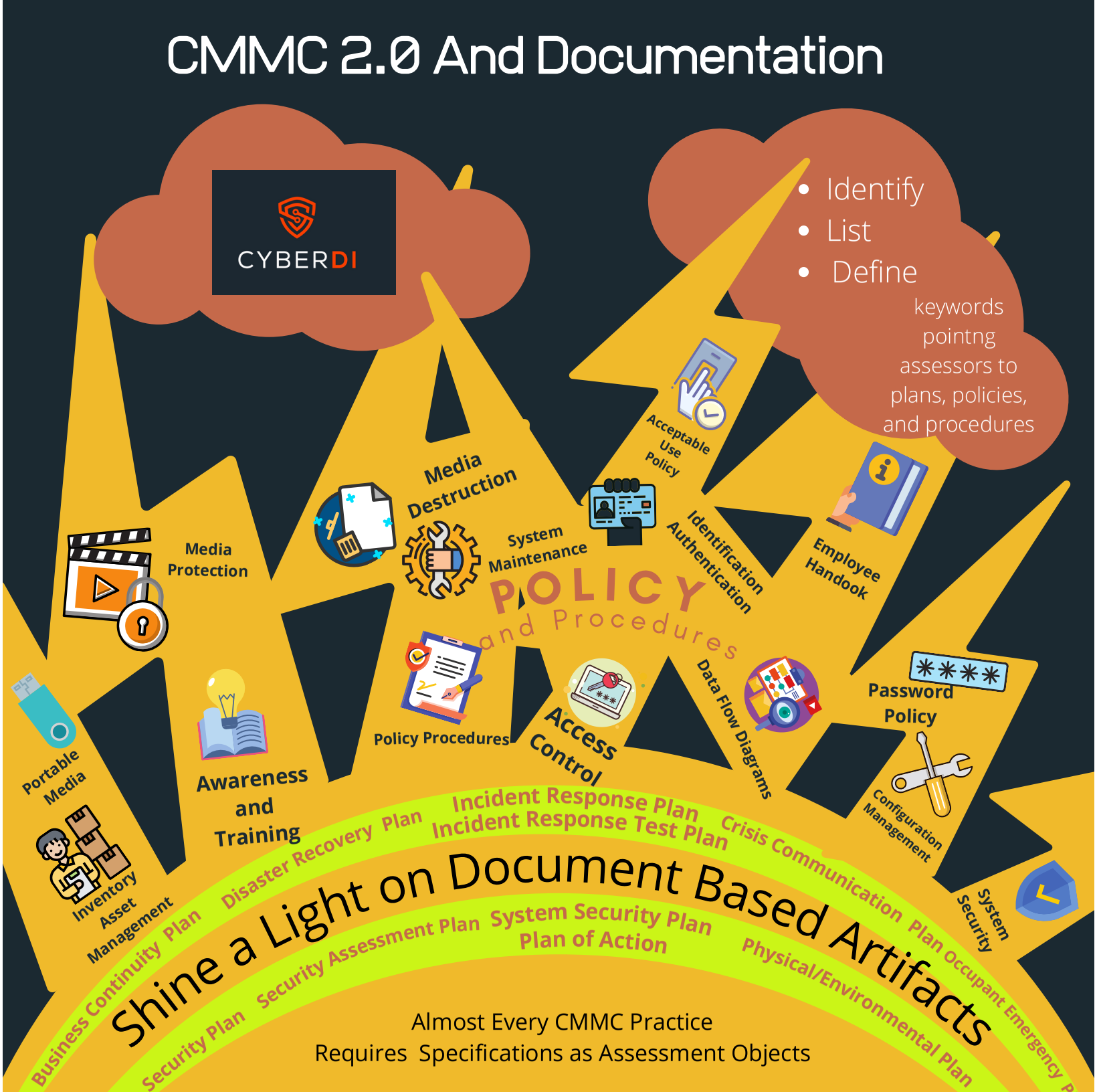
Provenance

where data originated, how it was created, and by whom

CMMC ASSETS

CUI Asset-process, store, transmit CUI	Asset inventory, SSP, network diagram	In scope, Assess against CMMC Practices
Security Protection Asset-Protect CUI	Asset inventory, SSP, network diagram	In scope, Assess against CMMC Practices
Contractor Risk Managed Asset-can but not meant for CUI.Seperated	Asset inventory, SSP, risk based security plan, network diagram	In scope, not Assessed against CMMC if risk based policies and procedures protect assets. Boundaries checked
Specialized Asset-IoT, OT, Test Equipment, Restricted Systems may have CUI	Protected by risk based security policies, procedurees, anmd plans	
Out opf scope asset -NO CUI	Physically and Logically Seperated	Not assessed

CMMC 2.0 And Documentation



Pre-Requisites

- **Asset Inventory**
- **Network Diagram**
- **System Security Plan**
- **Shared Responsiobility Matrices**

CYBERDI

CMMC SCOPING

CYBERDI

CUI ASSET

Security Protection ASSET

Contractor Managed Risk ASSET

Specialized ASSET

Out of Scope ASSET

Documented in Asset Inventory

Documented in System Secuirty Plan

Documented in Network Diagram

Physically logically seperated

Assessed Using Applicable CMMC Practices

Assessed in Risk based Security Plans, Polices, and Procuedures

Not Assessed

CUI Assets

Process

Store

Create

used by assets to create, access, change, store, transmit, or destroy Controlled Unclassified Information

Assessed Using Applicable CMMC Practices

SPA

People

Technology

Facility

Security Protection Assets include the people and tools to protect CUI Assets. SPAs may or may not hold CUI and can include contractors

Contractor Risk Managed Assets

NIST-SP-800-171 is a standard. You may meet the CMMC Requirements nested in a risk based security plan

Capable of but not meant for CUI

Reviewed in SSP per CAL.L.3.12.4

Physical or Logical Separation Not Required

Assessor may review policies and procedures to ensure no CUI

Self Assessed Using Risk Based Security Plan

Risk Based Frameworks

- RMF
- CSF
- CIS
- COBIT
- GLBA
- CIS

CA.L2-3.12.4

Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

Specialized Assets

Gov Property

Internet of Things

OT

Restricted Info Systems

Test Equipment

Reviewed in SSP per CAL.L.3.12.4

Self Assessed Using Risk Based Security Plan

FCI and CUI

FCI = Level One

CUI = Level Two

In scope on same system

- Contractor may choose one assessment and define FCI/CUI boundaries
- A contractor may choose to have each system assessed
  - self-assess FCI systems
  - self-assess or third party CUI systems

In scope on two systems

External Service Providers

Can fall in scope

If So

Shared Responsibility Matrix Required

Evaluate other Compliance Standards

Use Vendor Agreements as Evidence

CUI Marking Guidance

PROTECT FROM CUI UNAUTHORIZED DISCLOSURE

2016 CUI Marking Handbook v1.1

CYBERDI

Control Marking
Required

- BOLD
- CAPITALIZED

CUI Designation Indicator

DoD requires an indicator block to meet CFR 32 part 2002 req

- Controlled by: [Name of DoD Component] (Only if not on letterhead)
- Controlled by: [Name of Office]
- CUI Category: (List category or categories of CUI)
- Distribution/Dissemination Control:
- POC: [Phone or email address]

Five Required Items of CUI Designation Indicator

- Indicator of DoD component origination
- Indicator of Do Doffice origination
- CUI Category(ies)
- CUI Category(ies)
- Point of Contact

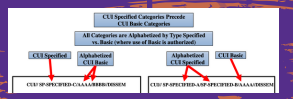
CUI Categories
Required if specified

CUI Basic
standard "flavor" of CUI.

CUI Specified
spells out additional requirments for protection by law, policy, regulations

Specified Not Higher Just Different

SInclude all categegories specified or not in banner marking



Limited Dissemination Control
Required by DoD Guidance

Limited Dissemination Control Markings are separated by adouble forward slash (//)

- No Foreign Dissemination (NOFORN)
- Federal Employees Only (FED ONLY)
- Federal Employees and Contractors Only (FEDCON)
- No Dissemination to Contractors (NOCON)
- Dissemination List Controlled (DL ONLY)
- Authorized for Release to Certain Foreign Nationals Only (REL TO USA, LIST)

If the law, regulation, or Government-wide policy is listed in CUI Registry as a Specified Authority, mark the CUI based in that Authority as CUI Specified and include that marking in the CUI Banner

Portion Marking

- optional in a fully unclassified document
- placed at the beginning of the portion
- must have contro marking, categories, LDC

Multiple Pages

Banner marking = Sum of all of the CUI markings in the document

Digital Media

- Alert holders to stored CUI
- Have Controling Marking
- Have Originator

Due to space may not be possible to include

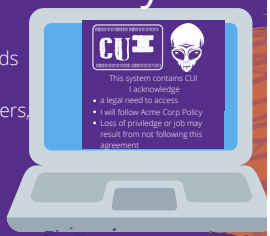
- CUI Category,
- Subcategory
- Limited
- Dissemination Control Markings.

Rooms

Alert personnel who are not authorized to access it

Have room marking procedures in CUI Policy

IT System



Use alternate marking methods on IT systems, websites, browsers, or databases approved in CUI policy

Mail

- Address packages with CUI to one person
- DO NOT put CUI markings on outside of an envelope or package
- Track the package

eMail

Banner Marking above text

Banner Marking above text when forwarding or responding

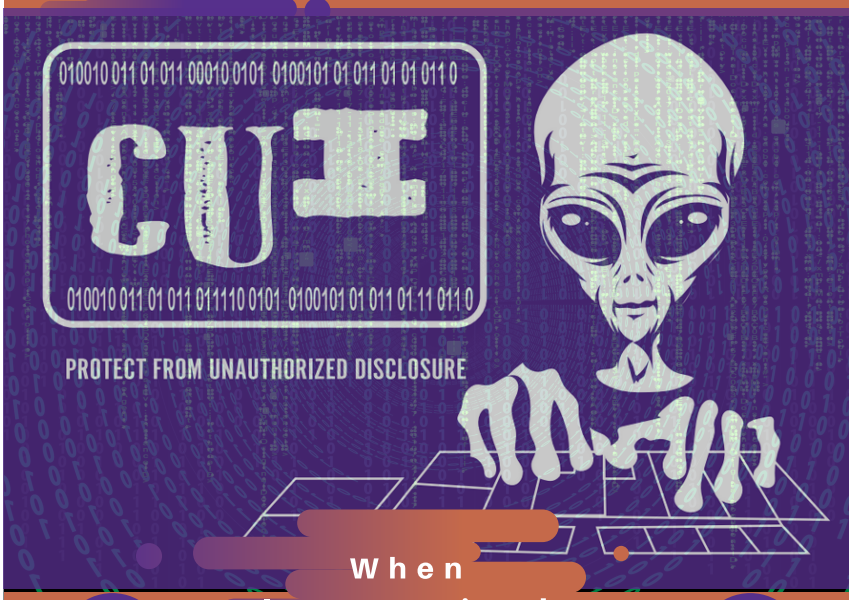
Legacy Markings

- Unclassified information marked as restricted from access or dissemination in some way
- or otherwise controlled
- prior to CUI Program.

ALTERNATIVE MARKINGS

Making Recipients Aware

CUI Notice 2020-02: Alternate Marking Methods



When Impractical

Quantity

Some systems may hold thousands to millions of records

Waiver

Agency Issued Limited Marking Waiver

Nature of Info

Data such as code, 3D models, CAD files, GCode that does not work with banner markings

Stop worrying about marking ALL the data and start worrying about systems that hold ANY of the data

Requirements

CYBERDI

- Designation Indicator
- Indicate CUI
- List specified Categories

If So

- Include laws and or regs that make it CUI-Specified
- Include limited dissemination controls

Or consider using metadata. Maybe provenance, who/when/where, a file gets made for large data sets

Scenario

Engineer sends folder containing files with CUI. Machinist gets a loginn splash screen

Alternative Markings

Do not need a CUI Indicator on Every Page

CUI banner marking may apply to the system and not a file

Consider the different laws around CUI Specified

Statements or banners work for emaol

Designated Indicator

Designating CUI occurs when an authorized holder

- Letterheads
- Logos
- Controlled by lines

Make A Statement

statements in splash screens often get used

Portable Media Different Alternate Rules

Next Episode

CYBERDI

DESTROYING CUI

CYBERDI

Authorized holders may destroy CUI when the agency no longer needs the information; and Records disposition schedules published or approved by NARA allow

CHAPTER 33 OF TITLE 44, U.S.C.

Unreadable | Indecipherable | Irrecoverbale

NIST-SP-800-88

GUIDELINES FOR MEDIA SANITIZATION

CUI NOTICE 2019-03

DESTORYING CUI IN PAPER FORM

Electronic

Clear: overwrite data, ATA commands, or facotry resets

Degaussing-Used for Purging Magentic Tape Hard Drives

Cyrptographic Erase-Destorying the key leaving data encrypted

Destroy: Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.

Hard Copy

Burning, cross-cut shredding, wet-pulping, melting, mutilation, chemical decomposition or pulverizing. (32 CFR 2001.47)

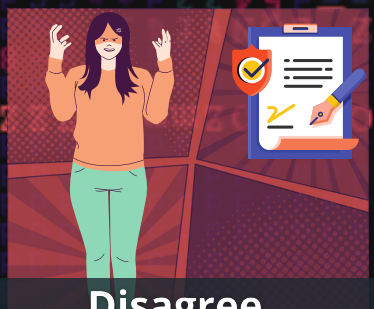
- **cross-cut shredders t 1 mm x 5 mm (0.04 in. x 0.2 in.) particles**
- **Pulverize devices with 3/32 inch screen**
- **Shred then recycle into paper**

CLEAR | PURGE | DESTROY

REDUCING INTERNAL RISK

Like all aspects of security, screening employees requires a continuous process

Poor Performance



Disagree with Policy

Argue with co-workers

Financial Distress

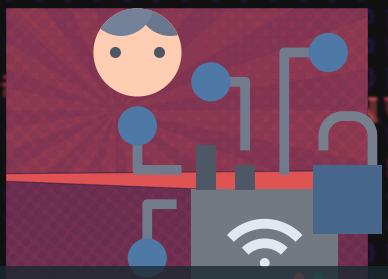
Unexplained Wealth

Strange Working Hours

Unusual Travel

Terminated Employee

New Hires



Attemps to bypass security

34% OF DATA BREACHES BY INTERNAL THREATS*

CYBERDI

Almost everyone who does bad thinks they are doing good

*2019 Verzon Breech Report

CYBERDI

CMMC

CYBERDI

Password Policies and Procedures

CMMC Requirements

3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.

Non-Federal Organizations Tailor Password Policies to their Needs

Say what you do, explain how you do it, prove it gets done.

Do you enforce Complexity?

DoD nor NIST publishes requirements for complexity or resetting

Just Guidance

NIST Handbook 162 = 12 characters.
NIST SP 800-63B =8 characters
DoD =15 characters, combo of capital and special characters no MFA

Password or Passphrase?

Length beats complexity. If users need to remember a passowrd include passphrases in your policy

Do you require Resetting?

Explain in policy if you require periodic resetting.
Make employees change passwords on reset

NIST Recommends getting rid of password complexity and expirations policies

No adding or changing one character to an old password

Do you use Multi-Factor Authentication?

Many CMMC Practices Require MFA

Privileged Users
Perform security or duties abiove normal employees

< MFA All Access

MFA Network Acccess >

Non-Privileged Users
Perform security or duties abiove normal employees

Can you Use a Password Manager?

The discussion section in NIST 171 seems to negate use of modern password manager technologies.
YOU CAN AND SHOULD USE PASSWORD MANAGERS

Think About Your Training Program!!

MFA

The Puzzle

Multifactor Authentication

Know | Have | Are

Privileged user
Does security and boss stuff.
Requires MFA 24/7
Local and Network

Non-privileged user-
Does stuff.
Requires MFA for Network and remote access

Identity-Proof of who you are

Authorize: Granting access after agreeing you are who you say you are

Access: Giving up the goods (hopefully to authorized users)

Key Terms

2 Good Moar Better

2FA
secondary proof like sms after password
Weakness: only one additional verification

MFA
multiple proof options: geolocation in network test biometric authenticator tokens. SMS.
Weakness: annoying

90% phishing attacks target credentials

NIST 171 requires two or more different factors to achieve access

Replay Attack

Tool Questions

- Ease of Use
- Ease of IT Roll-out
- Onprem/cloud
- total cost (COST)
- Policy Templates
- Log Automation
- One Time Authorizers

Copying deets of old log in ,tokens, or with old password

One time authorizers keep advesariers locked out

NIST SP-80-171 Rev 2 only requires replay resistant MFA on privileged accounts. Rev 3 will require it for all accounts

CHALLENGE

WHY MFA

Choose factors employees have comfort with using

Have a clear policy for employees to follow

Integrate with your access control audit log functionality. Know the capabilities of tools you have. Understand the defaults.

Include training and consider how handle reseeding MFA passwords and new devices

TIPS

81% of breaches caused by stolen or week passwords

73% of passwords are reused

123456 17% of passwords are 123456

Verizon 2019 Vulnerability Report

CMMC Practices

3.5.3
Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts

3.7.5
Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete

CYBERDI

WORKSTATIONS AND CONTROLLED ENVIRONMENTS

The Office

- Locked door acts as a physical barrier
- Clean Desk Policy
- MFA for network access for non-privileged users
- Log out after inactivity
- Obscure log in details upon access
- Lock away CUI if office open to others

Government Facility

- Policies and Procedures limiting portable storage devices
- Data transmission polices for hard copy CUI in transit
- Inherit the facility policy and procedure upon arrival until departure

CYBERDI

- Locked door acts as a physical barrier
- Clean Desk Policy
- MFA for network access for privileged users
- Log out after inactivity
- Obscure log in details upon access

- Requires tools such as as VPN or VDI
- No split tunneling
- Lock away CUI if office open

Family does not need visitor lob

Home Office

Even with the most mature remote policies, required encryption, and correct VDI deployment the coffee shop, and most public places, is not a controlled environment,

Coffee Shop

ALTERNATIVE SETTINGS NEED EQUAL SECURITY TO ORGANIZATION

Advanced Encryption Standard (AES)

Secure Hash Standard (SHS)

Digital Signatures (DSA, RSA and ECDSA)

Triple-DES Encryption Algorithm (TDEA)

CYBERDI

FIPS 140-2A

WHAT IS FIPS-140-2A VALIDATED ENCRYPTION?

A Government publication of encryption standards from the Federal Information Processing Standards in accordance with the Federal Information Security Management Act (FISMA) and approved by the Secretary of Commerce

WHAT IS A FIPS-140-2A VALIDATED MODULE?

FIPS 140-2a does not provide encryption or keys. Vendors can validate modules, part of the software encrypting data encrypting CUI or security to protecting CUI to the standard

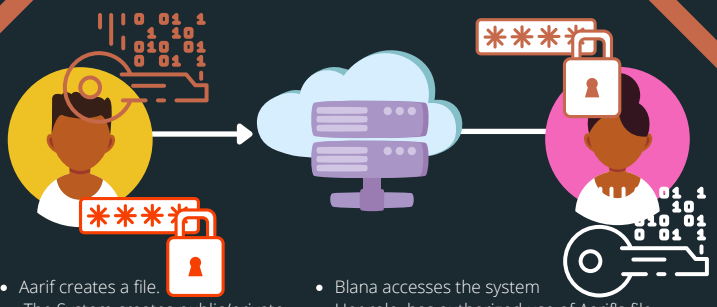
WHEN MUST FIPS-140-2A VALIDATED MODULES GET USED

FISMA dictates that U.S. government agencies must use FIPS 140-2 validated cryptography modules to protect data such as CUI classified at the moderate level

WHAT IS THE DIFFERENCE BETWEEN COMPLIANCE AND VALIDATION?

Compliant-Just the modules, often from a third party validated
Validation: Entire tool tested and validated at an accredited laboratory.

FIPS 140-2 requires hardware or software cryptographic modules use approved algorithms



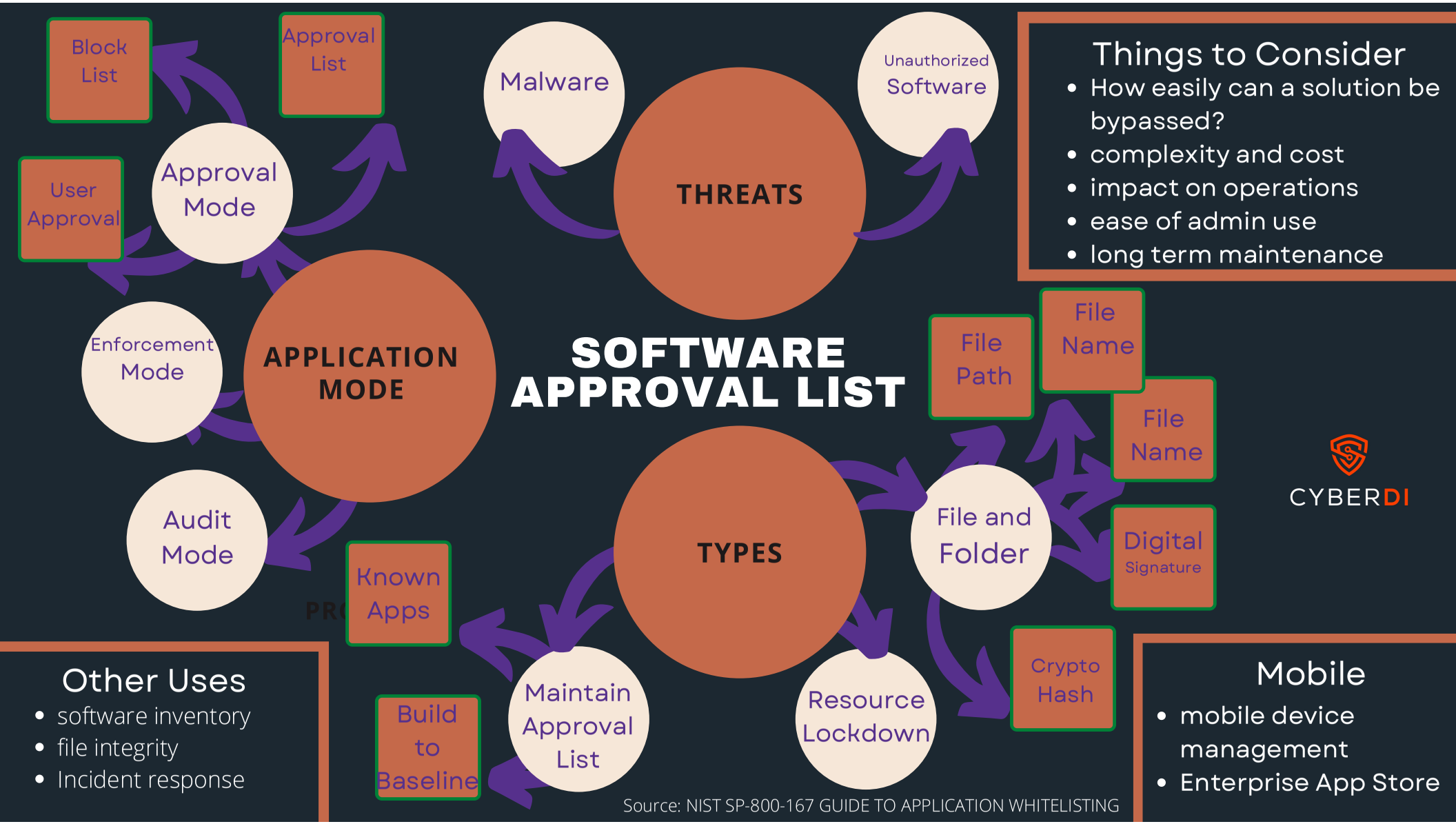
- Aarif creates a file.
- The System creates public/private key pair.
- Aarif gave Blanca, and anyone with her role access.
- Aarif's public key gets stored on the server. The private key on his device.
- The public key encrypts the file Aarif uploads with a symmetric key.

- Blana accesses the system
- Her role has authorized use of Aarif's file.
- Blanca downloads the file encrypted with a symmetric key.
- The private key on Blanca's device matches her public key in the symmetric key of the file
- The file opens

The system providers or privliged users never have access to keys in End-to-End Encryption

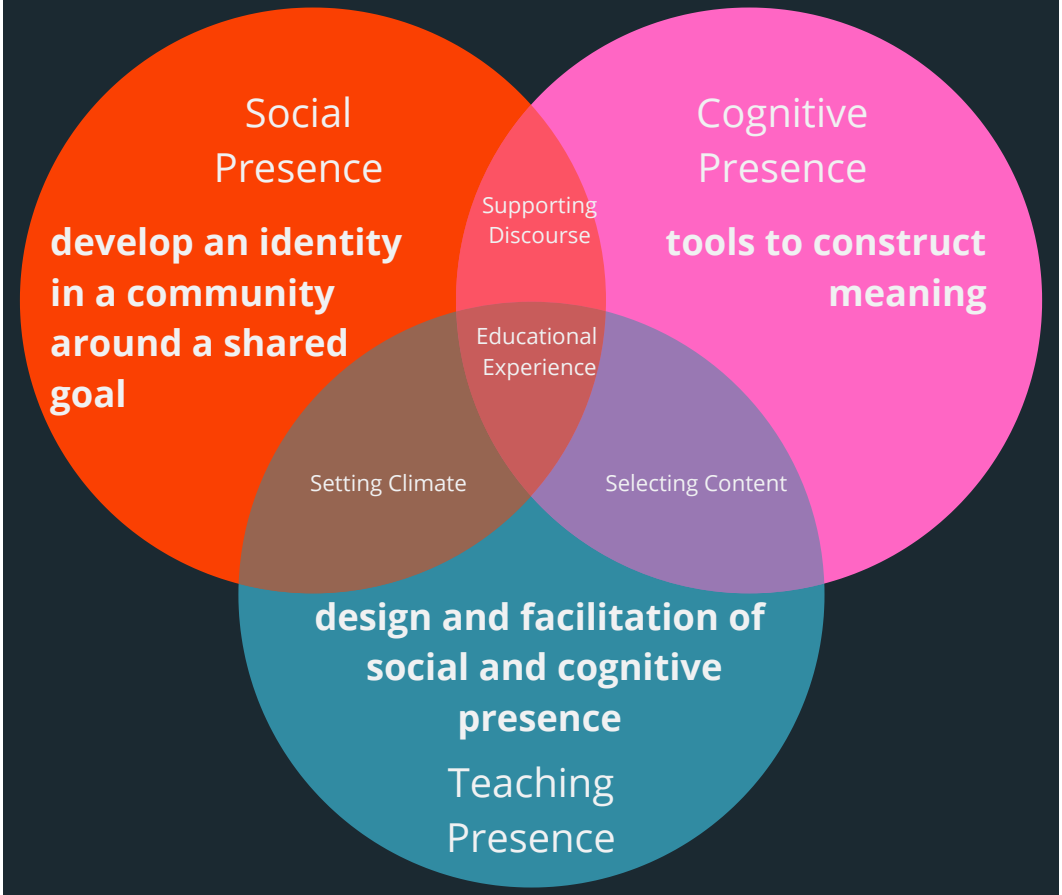
- **FIPS-validated cryptography required whenever encryption needed to protect CUI in accordance with NIST SP 800-171**
- **Digital CUI in Transit need encryption (files sending)**
- **Digital CUI at rest (files saved) needs encryption**
- **Portbale media devices (transit and rest) need encryption**
- **Online clouds and email need encryption (transit and rest)**
- **Devices such as routers inside physical security can use other encryption**
- **Many systems have a FIPS and not FIPS mode. Know the defaults**

Message Authentication (Triple-DES, AES and HMAC)


SOFTWARE APPROVAL LIST
APPLICATION MODE
Block List
Approval List
Approval Mode
User Approval
Enforcement Mode
Audit Mode
THREATS
Malware
Unauthorized Software
TYPES
Known Apps
Build to Baseline
Maintain Approval List
Resource Lockdown
File and Folder
File Path
File Name
File Name
Digital Signature
Crypto Hash
Things to Consider
How easily can a solution be bypassed?
complexity and cost
impact on operations
ease of admin use
long term maintenance
CYBERDI
Other Uses
software inventory
file integrity
Incident response
Mobile
mobile device management
Enterprise App Store
Source: NIST SP-800-167 GUIDE TO APPLICATION WHITELISTING

CYBERDI

Community of Inquiry



25 Principles of Cognitive Science

- Learn steps sequentially
- Active learning drives results
- Targeted feedback improves results
- Connect to prior knowledge
- Make a safe environment
- Keep it fun
- Learning takes rehearsal
- Reduce cognitive load
- Deliver content multiple times across modes
- Instructional Design: KISS
- Stories and case studies matter
- Vary the content and difficulty of tasks
- Make it emotional
- Create practice routines
- Interweave previous learning
- Encourage metacognition
- Assessments improve performance
- Summative assessments improve retention
- Authentic assessments improve retention
- Scaffold, but make it difficult

Predictable Navigation

- Read
- Write
- Participate

- Create mental models
- Require higher order thinking
- Failure is improvement
- Failure without feedback is useless
- Paper beats digital

Read about a topic. Write about what you read. Do something with what you read and wrote.

CYBERDI

Dr Lisa Lancor
Project Manager

Dr Lauren Tucker
508/ADA Compliance

Dr. Jeff Baldwin
Curriculum Writer, PI

Dr. Maureen McWhite
Curriculum Writer, PI

Vincent Scott
Curriculum Writer, PI

Paul Netopski

Technical Lead, PI

Lambo Publishing

Cloud Curriculum

Leslie Weinstein

CUI Curriculum Writer

Linda Rust

171 Curriculum Writer, PI

Dana Mantilla

Video Production

Leighton Johnson

CUI Curriculum Writer, PI

Shelly Weite-Bey

171a Curriculum Writer

Richard Dawson

RMF Curriculum Writer

Elvis Moreland

171a Curriculum Writer

Kelly Kendall

171a Curriculum Writer

Jill Lawson

7012 Curriculum Writer, PA

Karen Walsh

Legal Curriculum Writer

Carter Schoenberg

IATM Curriculum Writer

Shelby Scott

Curriculum Editor

Glenn Axelrod

Curriculum Writer

Mazz Media

Webinar Producer

Mark Lassof

Video Production

Jon Albright

Quality Assurance