DFARS 7012 / NIST 800-171 / CMMC Workshop

Addressing security frameworks through SSP, POA&M, and IRP

Adam Austin, MSIA, CISM, CISA
Cybersecurity Lead
Haight Bey & Associates/Totem Technologies
adam@haightbey.com
adam@totem.tech
https://www.linkedin.com/in/adam-austin-cybersecurity/

TOTEM

J31

F35

Totem.Tech

- Haight Bey Formed in 2014 from former Textron Systems employees, currently executes contractor logistics support (CLS) contracts for USAF
- Totem.Tech: “Cybersecurity Empowerment” services for small business peers
  - Bootstrap continuous self-assessment program
  - Emphasize user and administrator training
  - Leverage free and open-source technology
- Cybersecurity Lead—Adam Austin
  - MSIA, CISM, CISA, Security+
  - 10 yrs supporting Federal government cybersecurity assessments
    - DoD—US Army, Navy, Air Force
    - DHHS

Workshop Agenda

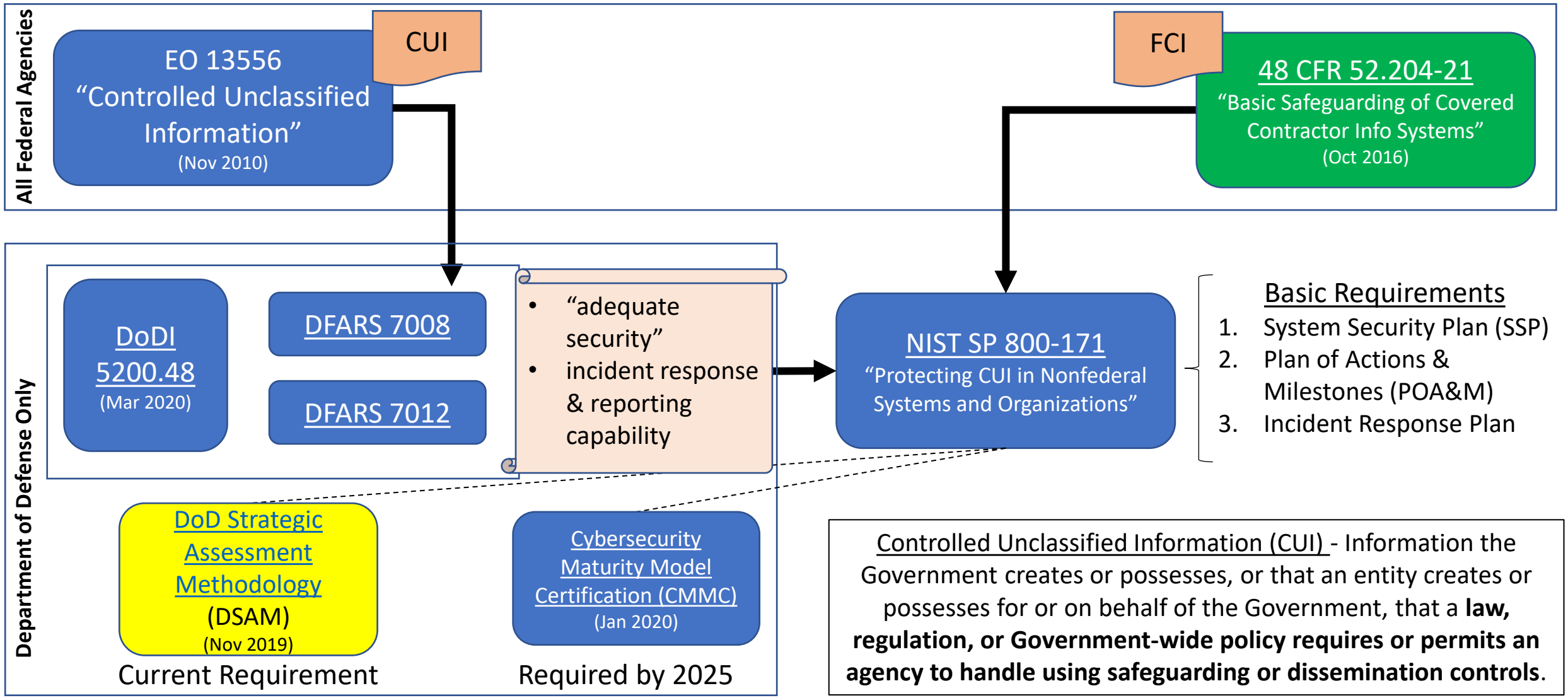
Topic #	Theme	Topic
1	Overview of Requirements	Overview of DFARS/CMMC cybersecurity compliance
2	Scoping your plan	CUI and System Inventory basics
3	Initial Assessment	The DoD 800-171 Assessment Methodology
4	Building an SSP	System Security Plan (SSP) requirements Introduction to Cybersecurity Program Planning
5	Incident Response Planning	Reporting Incidents—Obtaining an ECA certificate Incident Response Plan Basics

DFARS/800-171/DSAM/CMMC Overview

Topic 1:

- Understand relevant cybersecurity requirements
- Learn about the various cybersecurity implementation requirement timeframes

Regulatory Overview – Protect FCI & CUI



Controlled Unclassified Information (CUI) - Information the Government creates or possesses, or that an entity creates or possesses for or 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**.

FAR requires 17 safeguards

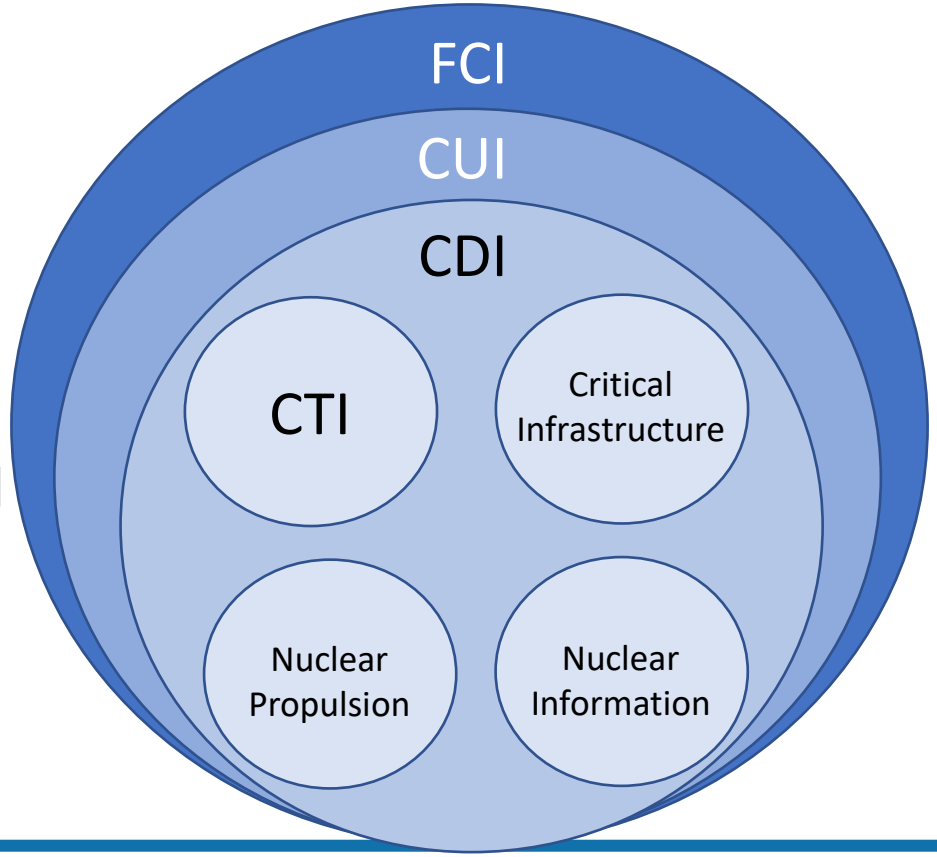
- 15 clauses comprising 17 basic requirements of **ALL** government contractors to protect any non-public data generated by or for a contract
- These 17 are all included in NIST 800-171
- Constitute all the CMMC Level 1 Practices

- https://www.acquisition.gov/content/part-52-solicitation-provisions-and-contract-clauses#id1669B0A0E67

DoD Federal Acquisition Regulation Supplement (DFARS)

- "Covered contractor information system": an unclassified IT system owned, or operated by or for, a contractor that processes, stores, or transmits covered defense information (CDI), e.g.:
- Controlled Technical Information (CTI):

- research and engineering data
- engineering drawings & lists
- specifications
- standards
- process sheets
- manuals
- technical reports
- technical orders
- catalog-item identifications
- data sets
- studies & analyses and related information
- software source code
- CDRLs



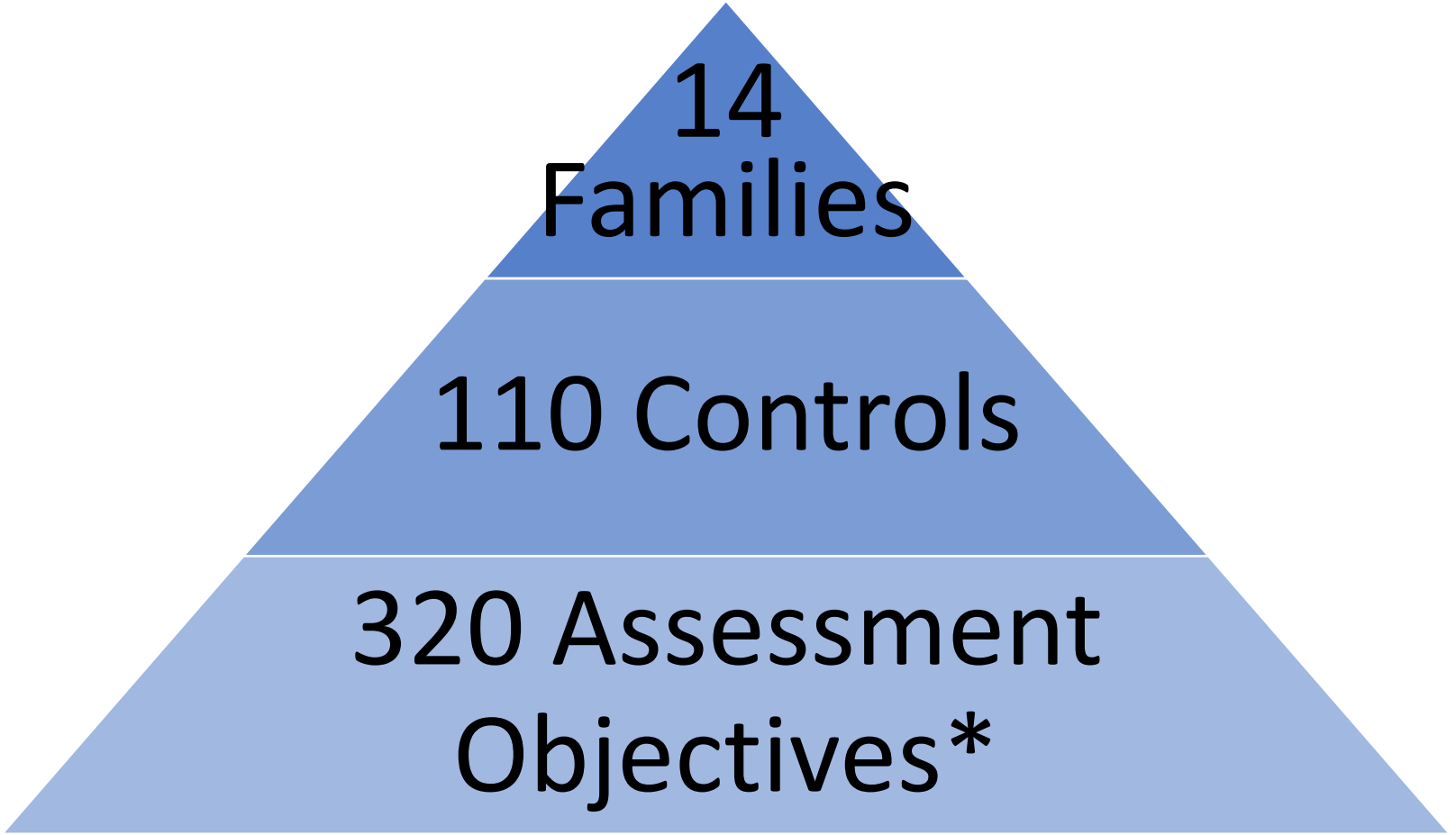
Many (most?) DoD contractors are "covered"

- Why: DoD has (correctly) determined its supply chain is a source of unacceptable risk
- If the contract specifies Contract Deliverable Requirements Lists (CDRL), your organization is likely covered
  - Only the IT systems that process CUI
  - E.g. CAD systems, MS Office systems used to develop Tech Manuals
  - Includes "cloud"-based IT systems—need FedRAMP approval
- Example of IT system not covered: G-suite tools (e.g. Google Drive) used only for corporate communications

What you must be doing right now

- DFARS clause 252.204-7012
  - **Adequate security**: The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017.
    - Operational, managerial, and technical cybersecurity requirements for IT system
  - **Cyber incident reporting**: Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.
    - Access to site requires ECA medium-assurance certificate (purchased by contractor), or CAC card

SP 800-171 Controls



*We refer to Assessment Objectives as “Organizational Actions”

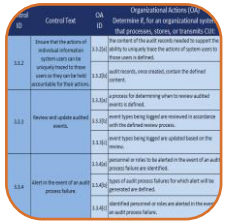
DoD Contractors w/CDI need to implement a cybersecurity program:

1. Gather existing system security plans (SSP)
2. Perform gap assessment against 800-171
3. Modify SSP accordingly; develop new policies/processes, written documentation for N/A controls
4. Develop and implement a capability to report cyber incidents
5. Develop and execute a Plan of Action and Milestones (POA&M) to fix residual gaps
6. Create and engage a continuous monitoring process

TOTEM

DON’T PANIC

DFARS Cybersecurity Compliance means “Implementing” 3 things:



Develop and Approve a 800-171-based System Security Plan (SSP)

Develop and Execute a Plan of Actions and Milestones (POA&M)

Develop and Implement a Cyber Incident Reporting Capability

TOTEM

Good News!

You create your SSP

- Create sensible custom policies

Lots of policy resources to draw from

- US Gov't
- SANS
- ACSC

Free and/or open-source tech options

- NetMon Freemium
- Security Onion
- GoPhish

TOTEM

Two Compliance Regimes

- DoD 800-171 Strategic Assessment Methodology
  - Current regime—being emphasized! (https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=202009-0750-001)
  - Process CUI? Perform self-assessment and submit score to DoD
  - DCMA/DCSA conducting "higher confidence" audits
- CMMC
  - Released in January 2020; C3PAO accredited in 2020?
  - Phased incorporation into **ALL** DoD contracts starting sometime in 2021
  - Certification required for contracts

Will supposedly be
"***complimentary and concurrent*** "

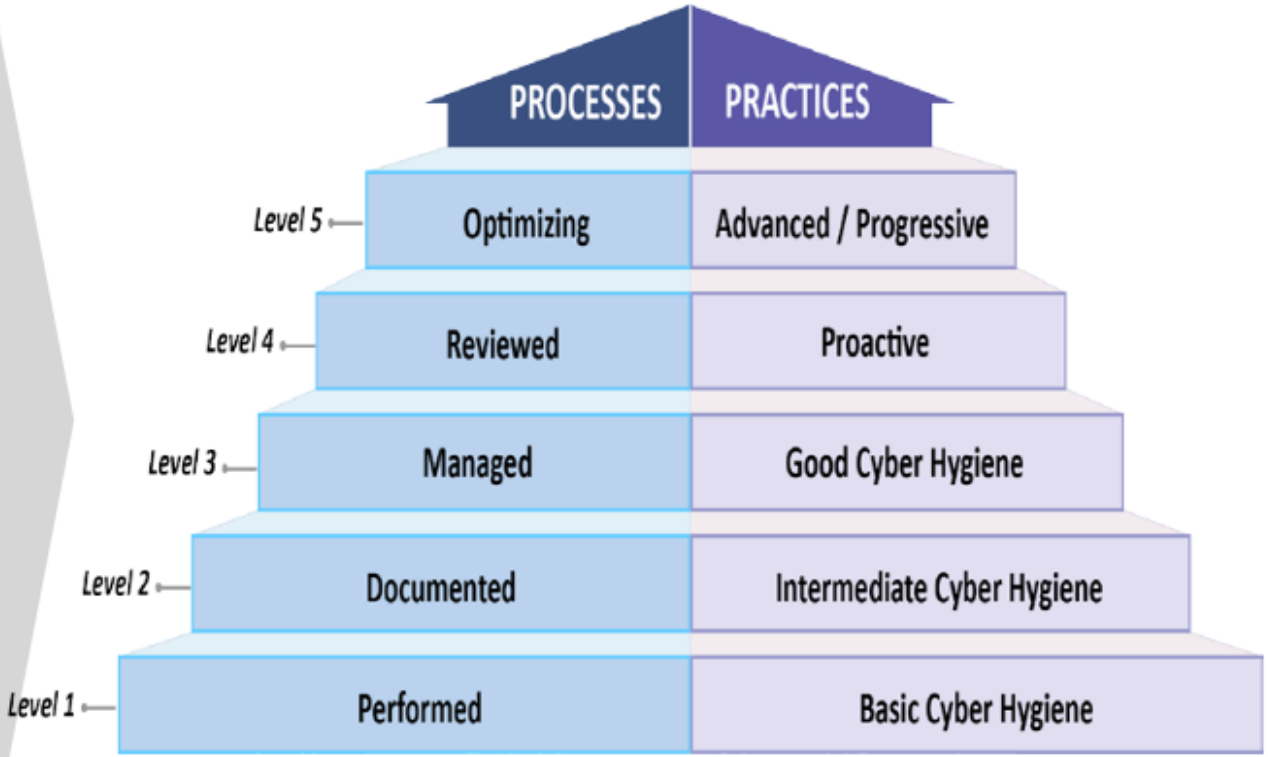
CMMC Basics

- License to operate: CMMC Certification required to propose to/execute DoD contracts
- Phasing in ~10 RFP in 2020 affecting ~1500 contractors; (starting with nuclear arsenal and missile defense?)
- All other new contracts phasing in CMMC through 2025
- CMMC third-party assessment organizations (C3PAO) responsible for issuing certifications

17 Capability Domains (v1.0)

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

CMMC Model with 5 levels measures cybersecurity maturity



CMMC by the numbers

	Level 1	Level 2	Level 3	Level 4	Level 5
Who?	All contractors	Some CUI processors	All CUI processors	APT-targeted organizations	APT-targeted organizations
What?	17 Practices (FAR 17)	72 Practices (includes some 800-171)	130 Practices (all of 800-171 + 20 additional)	156 Practices (includes enhanced assessment objectives from 800-171B)	171 Practices (includes enhanced assessment objectives from 800-171B)

Interested in knowing more about these additional 20 Practices?
https://www.totem.tech/cmmc-nist-800-171/

CMMC Maturity Levels

Maturity Level	Assessment Objective: "Does the organization…"	Nutshell
1. Performed	perform the practice?	Do it
2. Documented	perform the practice **AND** have a written process and policy?	Do it and document it
3. Managed	perform the practice **AND** have a written process and policy **AND** establish, maintain, and resource a plan demonstrating the management of activities for practice implementation, to include information on missions, goals, project plans, resourcing, required training, and involvement of relevant stakeholders?	Do it, document it, demonstrate resources for it
4. Reviewed	perform the practice **AND** have a written process and policy **AND** establish, maintain, and resource a plan demonstrating the management of activities for practice implementation, **AND** review and measure practices for effectiveness, to include the ability to take corrective action when necessary?	Do it, document it, demonstrate resources for it, measure its effectiveness and fix it
5. Optimized	perform the practice **AND** have a written process and policy **AND** establish, maintain, and resource a plan demonstrating the management of activities for practice implementation, **AND** review and measure practices for effectiveness, to include the ability to take corrective action when necessary, **AND** standardize and optimize process implementation across the organization?	Do it, document it, demonstrate resources for it, measure its effectiveness and fix it, automate it and have feedback loops for it across the enterprise

Scoping Your Plan

Topic 2:

- Learn how to develop a CUI and Systems Inventory

How do you know what's CUI?

- DoDI 5200.48: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF?ver=2020-03-06-100640-800
  - 3.7[e]:"CUI will be identified in SCGs [Security Classification Guide] to ensure such information receives appropriate protection."
  - 5.1[e]:"The program office or requiring activity must identify DoD CUI at the time of contract award…"
  - 5.3[b]:"…protective measures and dissemination controls…will be articulated in the contract, grant, or other legal agreement, as appropriate."
- DoD CUI Registry: https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/CUI/Forms/AllItems.aspx

Potential Indicators of CUI

- Markings
  - `UNCLASSIFIED` – although not always controlled!
  - `UNCLASSIFIED//FOUO` – probably controlled
  - `CUI`
  - `CONTROLLED`

- Distribution Statements:
  - "DISTRIBUTION STATEMENT C. Distribution authorized to U.S. Government agenciesand their contractors (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office)."
  - https://www.darpa.mil/attachments/Distribution%20Statements%20on%20Technical%20Documents-%20updated.pdf
- ITAR / EAR -- may or may not be, depends on contract
  - https://www.archives.gov/cui/registry/category-detail/export-control.html

CUI and IT System Inventory

- System Identification—for who, where, why
- System Operational Status—operational, under development, under modification
- General System Description—use cases
- System Environment Description—overview of technologies processing info
- System Interconnections/Information Sharing—table with following elements:
  - Connection
  - Info shared/use case
  - Sensitive info shared (CUI, PHI, IP, etc.): Y/N
  - Encryption mechanism
  - Authentication mechanism
  - SLA needed? Reference
- System Diagrams
- System Inventory

Two options for scoping the SSP:

1. Isolate CUI to a separate information system, and only apply adequate security to those processes, procedures, components

2. Co-mingle CUI and other organizational data, and apply adequate security to entire organizational information system

Initial Assessment

Topic 3:

- Perform an initial compliance assessment of your organizational systems

800-171 Strategic Assessment Methodology

- Scoring system for each of 110 controls
  - Weighted value subtracted from 110 for each non-compliant control
  - Can result in negative score
- At minimum, contractors required to self assess and report score and estimate date of full implementation to SPRS
  - Our knowledge base guide to score submission: https://www.reddit.com/r/TotemKnowledgeBase/comments/huv42x/latest_memo_on_dibcac_800171_assessment_updates/
  - Constitutes “Low” level of confidence
- For higher confidence, DCMA conducts audits
  - Medium: off-site review of SSP
  - High: on-site assessment of cybersecurity program using 800-171A

Building an SSP

Topic 4:

- Learn the basics of developing and implementing a System Security Plan (SSP)

Principles of good security policy

- Scalable
  - Is this statement simple, readable, concise, and measurable?
  - Is this statement repeated in another document?
  - Does this statement limit technology options, growth, or expansion?
- Auditable/assessable
  - Can an assessor verify implementation by:
    - interviewing organizational personnel?
    - examining or inspecting systems or documentation?
    - testing safeguards, processes, configurations, systems?

Example security policies

- Control 3.10.6:
  - Enforce safeguarding measures for CUI at alternate work sites.

3.10.6[a]	safeguarding measures for CUI are defined for alternate work sites.
3.10.6[b]	safeguarding measures for CUI are enforced for alternate work sites.

- "Discussion" from 800-171:

  Alternate work sites may include, for example, government facilities or private residences of employees. Organizations may define different security requirements for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites.

  NIST Special Publications 800-46 and 800-114 provide guidance on enterprise and user security when teleworking.

Example security policies (2)

- Addressing 3.10.6[a] *safeguarding measures for CUI are defined for alternate work sites*:
  - "Employees may work from home or other remote locations, but **shall** only process company information on a company-provided workstation. This type of remote work **shall** be authorized by the employee's supervisor. Remote employees **shall** only connect to the company network through the company-hosted Virtual Private Network (VPN). Remote employees **shall** only establish remote VPN connections through secured Internet connections, such as password-protected home networks, never using open or "public" Wireless Access Points."

  - "The safeguarding measures for CUI are defined in the company Acceptable Use Policy. See document "Company_AUP_Rev1.docx". "

Example security policies (3)

- Addressing 3.10.6[b] *safeguarding measures for CUI are enforced for alternate work sites*:
  - “Employees authorized for remote work are given company-provided workstations. Prior to connecting to the company Virtual Private Network (VPN), remote-work employees are required to submit to the company IT administrators the IP address of the network they are attempting connection from. The VPN, established by the company gateway firewall, filters VPN connection attempts by MAC and IP address and only allows company-owned machines to connect from authorized external networks. See the attached screenshot showing the VPN connection filter configuration.”

Example security policies (4)

- Hybrid approach:

3.1.17[b]	wireless access to the system is protected using encryption.

"Wireless access to the company IT system **shall** only be available through company-controlled Wireless Access Points (WAP). WAPs **shall** be configured to require passwords and transmit using the WiFi Protected Access II (WPA2) protocol engaging AES encryption. Wired Equivalence Protocol (WEP) and WiFi Protected Setup (WPS) **shall** be disabled.

The company has two password-protected WAPs, meshed together to provide common authentication, and WPA2 is engaged, with WEP and WPS disabled. See the attached screenshot which shows the security configuration settings of the WAPs."

Incident Response Planning

Topic 5:

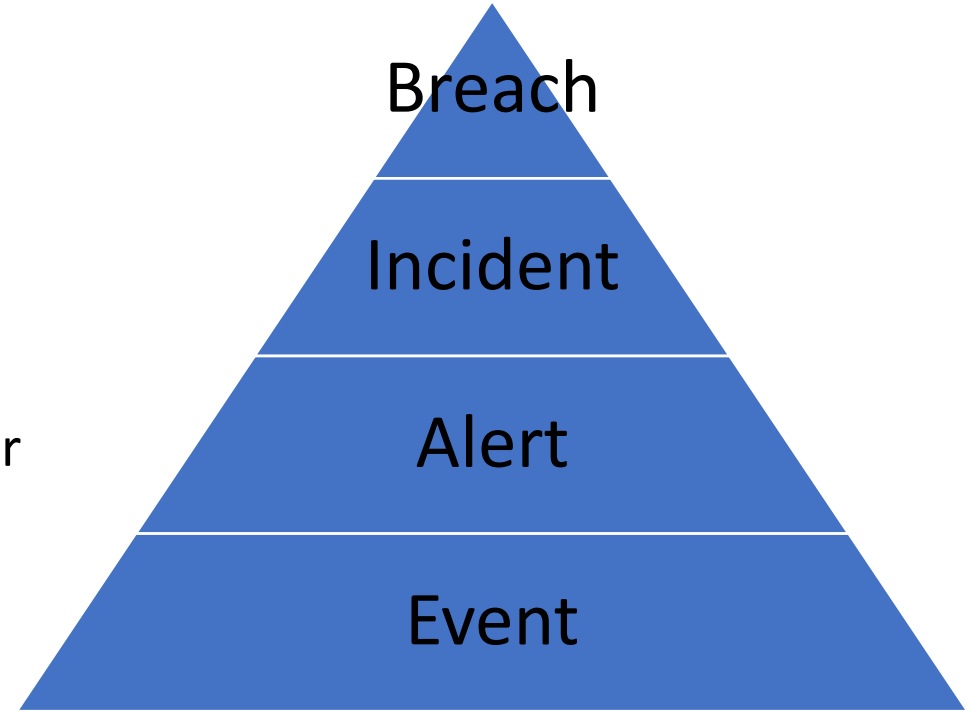
- Why you need an External Certificate Authority (ECA) cert and how to procure it
- Learn the requirements for Incident reporting
- Create a custom Incident Response Plan for your organization

ECA Certificates and Incident Reporting

- Obtain ECA certificates from one of two DISA vendors: https://public.cyber.mil/eca/
  - ~$100/year
  - Smart card, USB stick, saved to computer
  - Takes about a week—must snail mail notarized letter
- Reporting done here: https://dibnet.dod.mil/portal/intranet/
- Incident Report Template available in Totem templates page

Incident Response—Definitions

- **Event**: any observable occurrence in a digital ecosystem or computer network.
- **Alert**: event having a security context usually generated from threat detection assets or threat hunting routines.
- **Incident**: signifies a security control failure, or a violation, or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices
- **Breach**: incident where we know or suspect unauthorized access to protected information.

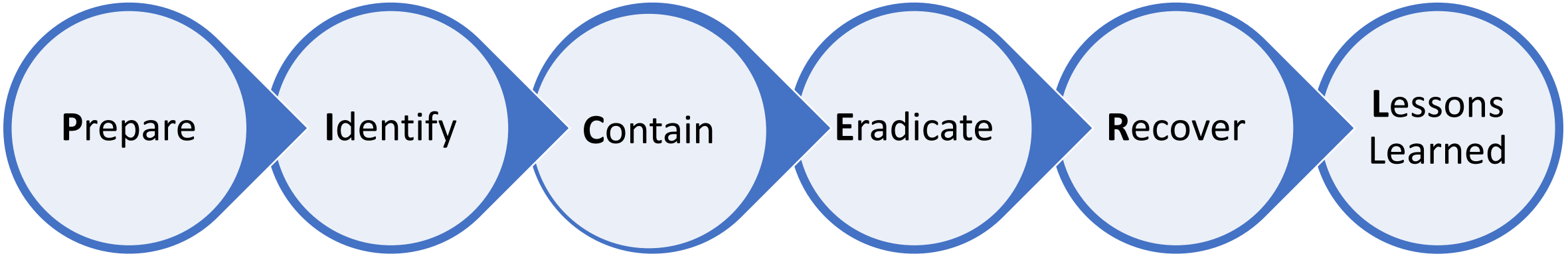


Example of an incident

1. An organization's server generates an event that indicates a failed logon for an administrator account; that event log is sent to a Security Information and Event Management (SIEM) server.
2. The SIEM creates an alert because the failed logon came at 3:00 AM, off hours for the organization, when administrators normally would not be working.
3. Upon investigating the alert, the security operations team realizes multiple failed logons to multiple different machines occurred around the same time, originating from a single workstation in the Engineering department, and that workstation also had inbound connections to it from an IP address outside the organization. The security operations team classifies the circumstance as an incident, and the organization CSIRT begins Incident Response.
4. After isolating the workstation from the network and determining that it had been infected with malware allowing an adversary a persistent remote connection to the workstation, and that the workstation housed engineering data considered CDI, the organization classifies the incident as a breach.
5. After containing the incident and determining exactly what CDI may have been compromised, the organization files an Incident Report with the DoD.

Incident Response Planning (IRP)

- PICERL
- There is an IRP template on the Totem templates page



Prepare

- 2nd most important phase (Contain is most important)
- Contact information for the ISO
- Contact information for the CSIRT
- List of responsibilities for the ISO
- List of responsibilities for the CSIRT
- List of recovery metrics: MTD, RTO, and RPO
  - team must understand the time parameters they need to meet during IR
- List of individuals within the organization to share IR information with
- Contact information for external entities to share IR information with
  - DoD; other US government officials, e.g. the FBI
- Instructions for exercising the IRP

Identify

- Assess the alert and classify it as an official “incident”, if necessary
  - First, rule out the possibility that the alert is the result of an authorized change
  - Draw the team’s attention to Indicators of Compromise (IOC) and attack tactics, techniques, and procedures (perhaps include these lists in this section or in an appendix)
- Memorialize and share information, including
  - Format of notes, collaboration tools, encryption requirements
- Collect and store evidence

Contain

- **The most important phase**
- Methods/steps will be unique to organization, but playbooks can help
- General guidelines:
  - Reminders to the team on effective containment strategies: inventory assets, detect, deny, disrupt, degrade, deceive, and destroy
  - Instructions on team relief, as containing the damage may mean long days for the team. Team members need to be sharp, so some rest periods are mandatory.
  - If it appears containing the problem will take longer than the RTO (see above), leadership must be informed so they can prepare alternate means of meeting the organization's IT needs

Eradicate

- Again, these steps are unique to the organization, and may be ad hoc
- SANS Playbook development resource: https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1559689083.pdf
- Canned playbooks: https://www.incidentresponse.com/playbooks/

Restore

- Checklists!
  - procedures for allowing a compromised IT asset to return to the system
  - restoration priority checklist
    - E.g.: domain controller must be up for account logins to work, especially if DC supports MFA
  - procedures for ensuring the IT system and data are back to normal operations, i.e. a “system checkout”

Lessons Learned

- Formal team meeting to discuss opportunities for improvement
- During this phase the IR report will be filed
- Capture results of exercises here

IR Resources

The **GOAT**: https://github.com/meirwah/awesome-incident-response

Phase	Description + link	Cost?
Prepare	How to obtain an ECA certificate	~$100/yr
Prepare	List of breach notification laws	Free
Prepare	SANS Incident Handling Forms	Free
Prepare/Identify	US-CERT incident scoring system	Free
Identify	SANS Digital Forensics cheat sheets	Free
Identify	Various Incident Response cheat sheets	Free
Identify	Info sharing US CERT Traffic Light Protocol	Free
Identify	Comparison of Endpoint Detection and Response (EDR) tools	Cost
Identify	Comparison of free digital forensics tools	Free
Identify	SANS SIFT Forensics Workstation	Free
Identify	AccessData Forensics Tool Kit (FTK) imaging and investigation	Cost
Identify	Wireshark packet capture tool	Free
Identify/Contain	MITRE ATT&CK Threat hunting framework	Free
Multiple	SANS IR playbook creation	Free
Multiple	French CERT IR playbooks	Free
Lessons Learned	MITRE IR exercise playbook	Free
Lessons Learned	CIS Six tabletop exercise scenarios	Free
Lessons Learned	More incident response scenarios	Free

Free E-Book

Price: ~~$49~~ FREE

Email: info@totem.tech

Subject: Free EBook

TOTEM

Thank you!

Totem Technologies
1972W 2550S Suite B
West Haven, UT 84401

(888) 379-0509

adam@totem.tech jackie@totem.tech christian@totem.tech

https://totem.tech

https://www.linkedin.com/company/totem-tech/

TOTEM