Cybersecurity Requirements in US Federal Government Contracts

SAME Small Business Conference

02-MAR-2020

Fathom Cyber
Defensible Cybersecurity Strategists

About the Speaker:

James ("Jim") Goepel

- CEO and General Counsel of Fathom Cyber
- Professor of Cybersecurity at Drexel University's Thomas R. Kline School of Law and LeBow College of Business
- Board Member, Treasurer, and Chair of Budget Committee, Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB)
- JD and LLM, George Mason University
- BSECE, Drexel University

Speaker Disclaimers

Information provided in this presentation does not, and is not intended to, constitute legal advice. All information available in this presentation is for general informational purposes only.

The views expressed in this presentation and verbally by the speaker are his own personal opinions and do not necessarily constitute the views or legal positions of his employer, clients, or the Cybersecurity Maturity Model Certification Accreditation Body.

Fathom Cyber
Defensible Cybersecurity Strategists

USG, Contractors, and Critical Infrastructure are Being Breached

- Office of Personnel Management breached
- Military and industrial intellectual property stolen
- US electrical grid nearly taken offline

Chengdu J-10 vs F-16

Fathom Cyber
Defensible Cybersecurity Strategists

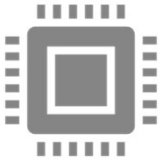
Some Agencies Offering Guidance to Contractors and Others

- Department of Energy Cybersecurity Capability Maturity Model (C2M2) – Developed 2014
- Comprised of three different models:
  - C2M2
  - Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
  - Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2)
- Not mandatory – instead, it is guidance meant to help DoE contractors and those in critical infrastructure supply chain to improve their cybersecurity maturity.

USG has a History of Taking Cybersecurity Seriously

Cybersecurity requirements come in two forms:

* Software/hardware development
* Systems design and maintenance (including COTS)



Custom-developed software and hardware will have their own, unique requirements (e.g., testing against Open Web Application Security Project or other standards) defined in the contract which may need to be flowed down to subcontractors who are helping with the development process.

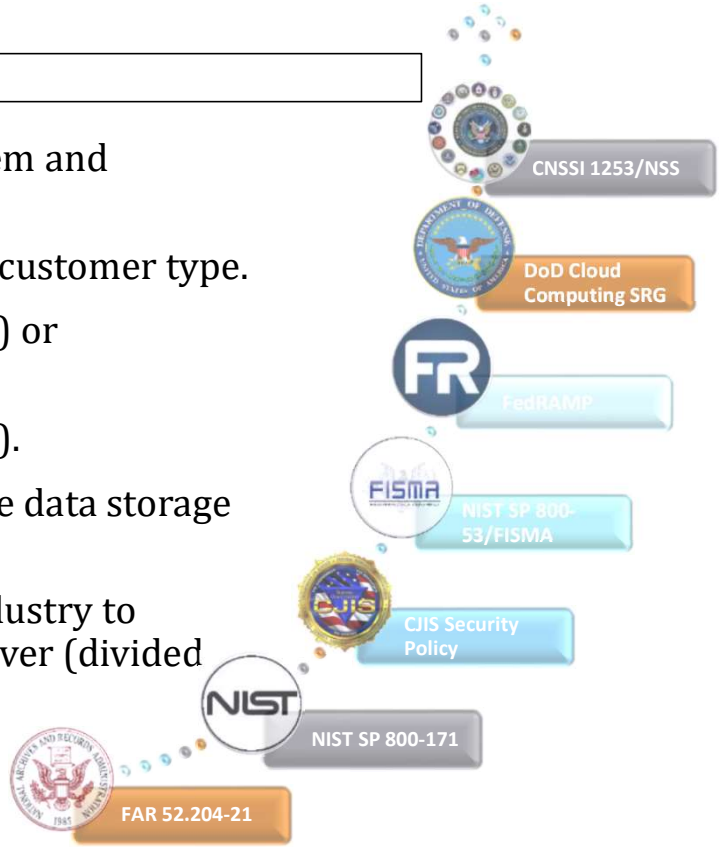
FAR and supplements focus on systems-level requirements, and this is the focus of this presentation as well.

Fathom Cyber
Defensible Cybersecurity Strategists

Current Federal Cybersecurity Controls Landscape†

†

- Federal Government follows escalating scale of controls, depending on system and information requiring protection.
- More controls are required at each successively higher level of security and customer type.
- Some security control regimes require Assessment and Authorization (A&A) or Authorization to Operate (ATO) by the Federal Government.
- State and Local governments follow Federal Government (usually voluntary).
- Some state & local governments have own security controls (e.g., no offshore data storage and/or non-U.S. citizen access to sensitive data).
- NIST Cybersecurity Framework (CSF) also provides guidance for private industry to assess and improve their ability to Identify, Protect, Detect, Respond & Recover (divided into 108 subcategories/controls).



*Some of these control schemes have multiple layers and may also not fully include all of the controls of the schemes below them. Plus, agencies may add more controls.

Fathom Cyber
Defensible Cybersecurity Strategists

FAR 52.204-21

Term	Definition
Covered Contractor Information System	means an *information system* that is owned or operated by a contractor that processes, stores, or transmits *Federal Contract Information*
Federal Contract Information	means unclassified *information*, not intended for public release (e.g., that would be labeled with a restrictive legend), that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as information necessary to process payments
Information	means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction [CNSSI] 4009)
Information system	means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of *Information* (44 U.S.C. 3502)
Safeguarding	means measures or controls that are prescribed to protect *Information Systems*.

Identifies **15 requirements** that ALL contractors must meet to work on Federal contracts.

These are the minimum requirements; additional requirements may be required on a contract-by-contract basis.

FAR 52.204-21 – Required Controls

Limit access to authorized users.	**Limit information system access to the types of transactions and functions that authorized users are permitted to execute.**	Verify controls on connections to external information systems.	Impose controls on information that is posted or processed on publicly accessible information systems.	Identify information system users and processes acting on behalf of users or devices.
Authenticate or verify the identities of users, processes, and devices before allowing access to an information system.	**Sanitize or destroy information system media containing Federal contract information before disposal, release, or reuse.**	Limit physical access to information systems, equipment, and operating environments to authorized individuals.	Escort visitors & monitor visitor activity, maintain audit logs of physical access, control/manage physical access devices.	Monitor, control, & protect org. communications at external boundaries & key internal boundaries of information systems.
Implement sub networks for publicly accessible system components that are physically/logically separated from internal ones.	**Identify, report, and correct information and information system flaws in a timely manner.**	Provide protection from malicious code at appropriate locations within organizational information systems.	**Update malicious code protection mechanisms when new releases are available.**	**Perform periodic scans of the information system and real-time scans of files from scans of files from external sources as files are downloaded, opened, or executed.**

Fathom Cyber
Defensible Cybersecurity Strategists

DFARS 252.204-7012 [Compliance]

- Applies to all DoD contracts and subcontracts (except if solicitation is solely for *commercial-off-the-shelf* products/services) and requires enhanced safeguarding of *covered contractor information systems* that contain *Covered Defense Information* (CDI)
- CDI is unclassified controlled technical information (CTI) or other information as described in the CUI Registry (http://www.archives.gov/cui/registry/category-list.html) that requires safeguarding/ dissemination controls AND IS EITHER marked or otherwise identified in the contract and provided to the contractor by DoD in support of performance of the contract; OR collected, developed, received, transmitted, used, or stored by the contractor in performance of contract.
- Mandatory flow-down clause in subcontracts at all tiers for *operationally critical support* **or** where subcontract performance will involve *covered contractor information system with CDI.*
- Must provide *adequate security* for covered systems with CDI; at minimum must have been compliant with NIST 800-171 not later than December 31, 2017.
- Can submit "alternative yet equally effective" controls to DoD CIO for approval.
- Must rapidly report *cyber incidents* on *covered contractor information systems* with *CDI*, or that affect the contractor's ability to perform *operationally critical support* under a contract and comply with other obligations essential to documenting the cyber incident.
- DoD will not currently certify that a contractor is compliant with NIST SP 800-171, and third-party assessments or certifications of compliance not required, authorized, nor recognized by DoD.

Fathom Cyber
Defensible Cybersecurity Strategists

DFARS 252.204-7012 [Cyber Incident Reporting]

- Contractors must report *cyber incidents* on covered contractor information systems with CDI, or that affect the contractor's ability to perform operationally critical support under a contract.
  - Upon discovery, must conduct a review for evidence of compromise
  - Rapidly report within **72 hours** directly to DOD via specified online portal (https://dibnet.dod.mil).
  - Must provide DOD-assigned incident report number to prime/higher-tiered subcontractor(s)
  - Must preserve and protect images of known affected images and systems for 90 days
  - Must provide DOD access to additional information or equipment necessary to conduct forensics analysis
  - Must submit any malicious software uncovered to DOD Cyber Crime Center (DC3), not the contracting officer
- A *cyber incident* that is reported by a contractor shall not, by itself, be interpreted as evidence that the contractor has failed to provide *adequate security* on its *covered contractor information systems*, or has otherwise failed to meet the regulation

Fathom Cyber
Defensible Cybersecurity Strategists

DFARS 252.204-7012 [Use of Cloud Services]

- If the contractor intends to use an external cloud service provider (CSP) to store, process, or transmit any CDI in performance of the contract, it must require and ensure that it meets security requirements equivalent to those in FedRAMP Moderate baseline.
- If after the award of a DoD contract, the contractor proposes to use cloud computing services in the performance of the contract, it must obtain approval from the DoD Contracting Officer prior to utilizing such cloud services.
- CSP must comply with requirements for cyber-incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber-incident damage assessment.
- Contractor must maintain within the U.S. or outlying areas all Government data that is not physically located on DoD premises, unless the Contractor receives written notification from the Contracting .Officer to use another location.

DFARS 252.204-7012 [Subcontracting]

- The Undersecretary of Defense issued a memo on January 21, 2019, addressing cybersecurity oversight as part of a contractor's purchasing system review.
- DCMA will leverage its review of a contractor's purchasing system in accordance with DFARS 252.244-7001, "Contractor Purchasing System Administration," to:
  - Review contractor procedures to ensure contractual DOD requirements for marking and distribution statements on DOD CUI flow down appropriately to its Tier 1 level suppliers.
  - Review contractor procedures to assess compliance of its Tier 1 level suppliers with DFARS 252.204-7012 and NIST SP 800-171.
- To ensure that a similar approach may be taken at companies for which DCMA does not administer contracts (such as the Secretary of the Navy's shipbuilding contracts), DOD will work with representatives of those communities to implement a similar solution.

National Archives & Records Administration [Civilian]

- Executive Order 13556 authorized the National Archives and Records Administration (NARA) to create a program for managing controlled unclassified information (CUI) across the executive branch.
- The NARA CUI Registry is an online repository for information, guidance, policy, and requirements on handling CUI (identifies/defines categories and subcategories of CUI).
- Procedures for use of CUI, such as marking, safeguarding, transporting, disseminating, reusing, and disposing of CUI.
- New *FAR* clause pending from NARA regarding CUI; expected to incorporate NIST SP 800-171.
- In the interim, most federal contracts contain FAR 52.204-21, "Basic Safeguarding of Covered Contractor Information Systems," requiring 15 basic security controls as part of a contractor's routine business practices.

Risks of Non-Compliance

- Liability under the Federal and State versions of the False Claims Act (FCA)
- *Universal Health Servs. Inc. v. United States et al. ex rel. Escobar*, 136 S. Ct. 1989 (2016):
  - "[L]iability can attach when the defendant submits a claim for payment that *makes specific representations* about the goods or services provided, but *knowingly fails to disclose* the defendant's noncompliance with a [*material*] statutory, regulatory, or contractual requirement."
- *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, 2019 WL 2024595 (E.D. Ca. May 8, 2019) – denied motion to dismiss allegations that Aerojet impliedly, but falsely, certified to the government that it was in compliance with DoD's cybersecurity rules (as well as NASA rules)
- *United States, et. al., ex. rel. James Glenn v. Cisco Systems, Inc.* (W.D.N.Y. July 31, 2019) – Cisco settled for $8.6M allegations it sold video surveillance systems with known vulnerabilities to federal and state government agencies
- Materiality factors include:
  - A contractor expressly certifying compliance,
  - The government requiring compliance as a condition of payment, and
  - Noncompliance that goes "to the very essence of the bargain" between the government and the contractor.
- **FCA liability includes three times the payment for the service—plus up to $21,916 in penalties per claim ≈ hundreds of millions in damages & penalties + significant reputational damage.**
- Even if no FCA liability attaches, failure to comply could result in suspension or debarment from future government business.

DoD has Recently Decided to be Even More Aggressive

- *"If we were doing all the necessary security controls, we wouldn't be getting exfiltrated to the level that we are. We need to level set because a good portion of our defense industrial base [("DIB")] doesn't have robust cyber hygiene. Only 1% of DIB companies have implemented all 110 controls from the National Institute of Standards and Technology. We need to get to scale where the vast majority of DIB partners can defend themselves from nation state attacks."*
- *"We cannot look at security and be willing to trade off to get lower cost, better performance or get something faster. If we do that, nothing works, and it will cost more in the long run."*
- *- Katie Arrington, CISO for Assistant Sec. Def. for Def. Acquisition, June 20, 2019 Announcing CMMC Program*

What is CMMC?

- Change to DFARS 252.204-7021 that will **require** a third-party assessment of a contractor's cybersecurity maturity based on the CMMC model.
- Targeted to be in 10 initial "pathfinder" contracts in September 2020.
- Will be integrated into additional contracts over a 5-year period.
- By 2026, CMMC requirements will be in all DoD contracts.

Who will be Subject to CMMC Requirements?

- Eventually, all contractors in the Department of Defense supply chain.
  - Prime Contractors
    - Subcontractors
      - Sub-subcontractors
        - …

Why did the DoD Create CMMC?

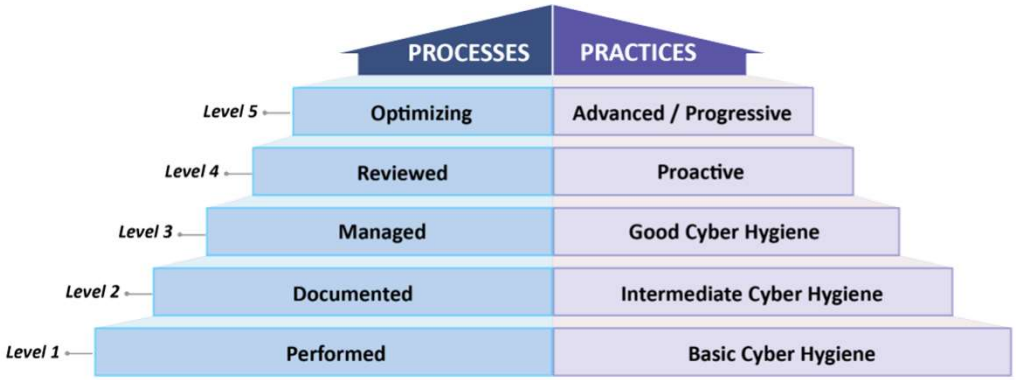
Cybersecurity incidents increase contract delivery costs, lengthen delivery timelines, and jeopardize business integrity.

Cybersecurity incidents have a negative impact on DoD's contractors:

- Malicious cyber activity cost the US economy between $57 billion and $109 billion in 2016 (The Council of Economic Advisors)
- $3 trillion in annual cybercrime losses in 2015, estimated to grow to $6 Trillion by 2021 (Cybersecurity Ventures)
- A new ransomware attack occurs every 14 seconds (Herjavec Group)
- Ransomware-as-a-service and open source malware are reducing barriers to entry for criminals (Sonicwall)
- The average data breach costs $3.9 Million worldwide, $8.9 Million in USA (Ponemon Institute)

How will my Organization's CMMC Maturity Level be Determined?

- CMMC model is divided into 17 "domains", each containing requirements for processes, capabilities, and practices.
- The organization contracts with an Assessor to assess the organization's maturity up to and including the org.'s desired Maturity Level.
- The Maturity Level assigned by the Assessor will be the <u>lowest</u> level achieved by the organization across all domains.
- **<u>No PO&Ms/POAMs</u>**



Fathom Cyber
Defensible Cybersecurity Strategists

Will all Contractors be Expected to be Maturity Level 5?

- In short, no.
- DoD has indicated that most of its contractors will only need to reach Maturity Level 1 because most do not have access to Controlled Unclassified Information ("CUI").
- Maturity Level 1 corresponds to existing requirements under FAR 52.204-21 and has been a requirement for any US Government contractor who has access to Federal Contract Information ("FCI").
- Contractors who have access to CUI will be required to meet CMMC Maturity Level 3 at a minimum, which is based on NIST SP 800-171.
- Only a relative few contractors are expected to need to meet Maturity Levels 4 or 5.

How Quickly will the CMMC be Rolled Out?

Total Number of Contracts with CMMC Requirement				
FY21	FY22	FY23	FY24	FY25
15	75	250	479	479

	Total Number of Prime Contractors and Sub-Contractors with CMMC Requirement				
	FY21	FY22	FY23	FY24	FY25
Level 1	895	4,490	14,981	28,714	28,709
Level 2	149	748	2,497	4,786	4,785
Level 3	448	2,245	7,490	14,357	14,355
Level 4	4	8	16	24	28
Level 5	4	8	16	24	28
Total	1,500	7,500	25,000	47,905	47,905

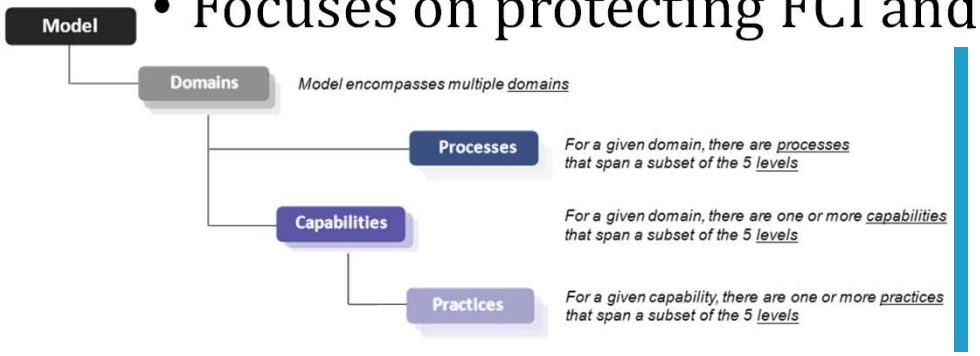
All new DoD contracts will contain the CMMC requirement starting in FY26

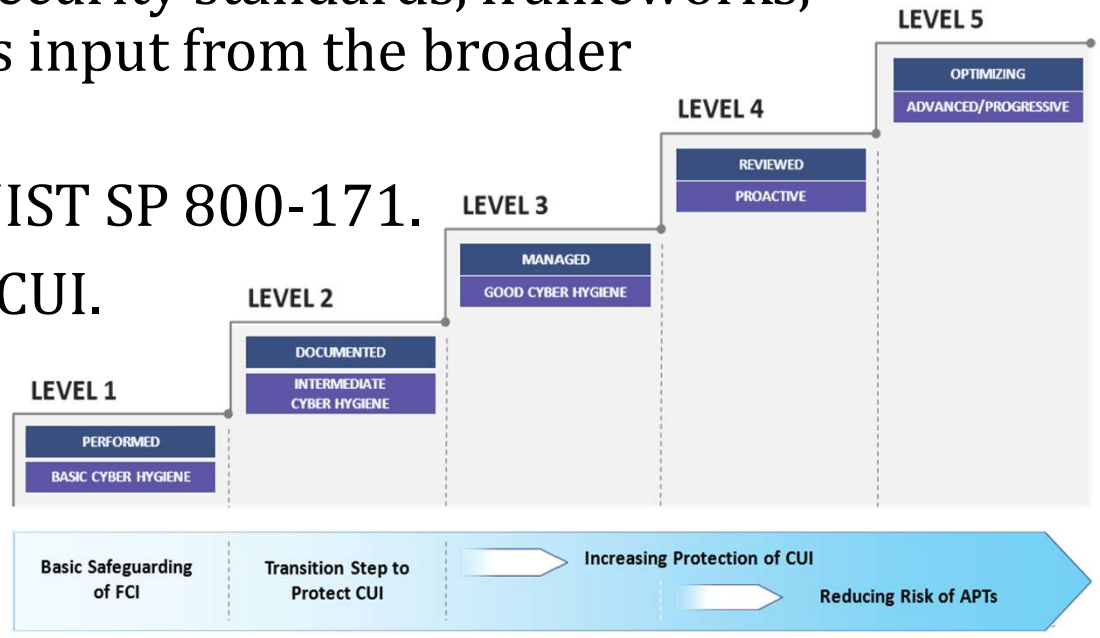
Source: Department of Defense, 1/28/2020. Subject to change.

Fathom Cyber
Defensible Cybersecurity Strategists

What is the CMMC Model?

- The CMMC Model defines a framework for measuring cybersecurity maturity with five maturity levels and aligns a set of policies and practices with the type and sensitivity of information to be protected and the associated range of threats.
- The model consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references, as well as input from the broader community.
- Based on FAR 52.204-21 and NIST SP 800-171.
- Focuses on protecting FCI and CUI.





CMMC Process Maturity Levels

Maturity Level	Maturity Level Description	Processes
ML 1	Performed	*There are no maturity processes assessed at Maturity Level 1.* *An organization performs Level 1 practices but does not have process institutionalization requirements.*
ML 2	Documented	Establish a policy that includes [DOMAIN NAME].
		Document the CMMC practices to implement the [DOMAIN NAME] policy.
ML 3	Managed	Establish, maintain, and resource a plan that includes [DOMAIN NAME].
ML 4	Reviewed	Review and measure [DOMAIN NAME] activities for effectiveness.
ML 5	Optimizing	Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organization units.

- CMMC recognizes that cybersecurity maturity requires more than just the implementation of certain technologies.
- To move beyond Maturity Level 1, organizations must have documented processes in place that govern their cybersecurity programs.
- Many organizations struggle with this.
- The documentation process frequently identifies areas where costs can be saved, and efficiencies realized.
- This can take significant time to implement and, although CMMC requirements may not apply to them now, organizations should begin creating appropriate documentation now.

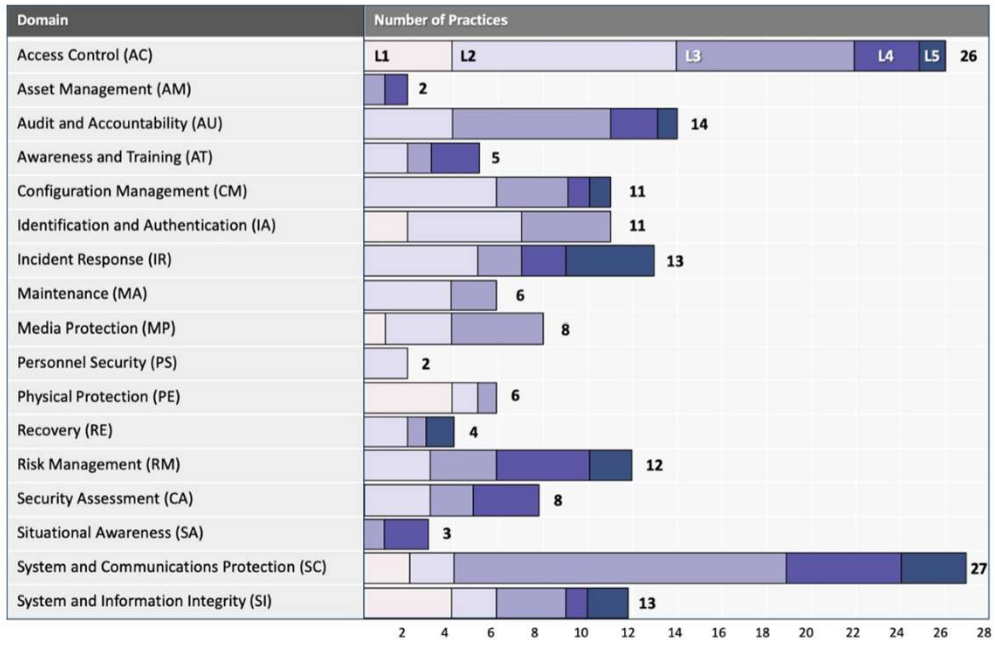
CMMC Capabilities

- Within each domain, CMMC requires that organizations address different capabilities.
- These capabilities aim to protect the organization, and DoD's FCI and CUI, from different threat types.

Domain	Capability
Access Control (AC)	• Establish system access requirements • Control internal system access • Control remote system access • Limit data access to authorized users and processes
Asset Management (AM)	• Identify and document assets
Audit and Accountability (AU)	• Define audit requirements • Perform auditing • Identify and protect audit information • Review and manage audit logs
Awareness and Training (AT)	• Conduct security awareness activities • Conduct training
Configuration Management (CM)	• Establish configuration baselines • Perform configuration and change management
Identification and Authentication (IA)	• Grant access to authenticated entities
Incident Response (IR)	• Plan incident response • Detect and report events • Develop and implement a response to a declared incident • Perform post incident reviews • Test incident response
Maintenance (MA)	• Manage maintenance
Media Protection (MP)	• Identify and mark media • Protect and control media • Sanitize media • Protect media during transport
Personnel Security (PS)	• Screen personnel • Protect CUI during personnel actions
Physical Protection (PE)	• Limit physical access
Recovery (RE)	• Manage back-ups
Risk Management (RM)	• Identify and evaluate risk • Manage risk
Security Assessment (CA)	• Develop and manage a system security plan • Define and manage controls • Perform code reviews
Situational Awareness (SA)	• Implement threat monitoring
Systems and Communications Protection (SC)	• Define security requirements for systems and communications • Control communications at system boundaries
System and Information Integrity (SI)	• Identify and manage information system flaws • Identify malicious content • Perform network and system monitoring • Implement advanced email protections

CMMC Practices

Although there are only 17 domains, the number of capabilities and corresponding practices increase as the organization matures and is able to handle larger amounts of or more sensitive CUI.



Fathom Cyber
Defensible Cybersecurity Strategists

Who will Oversee the Assessment and Certification Processes?

- Cybersecurity Maturity Model Certification Accreditation Body ("CMMC-AB").
- DoD asked industry to create a nonprofit, corporation-agnostic organization and the CMMC-AB was formed in January 2020.
- CMMC-AB is responsible for creating the CMMC Ecosystem, including:
  - Defining CMMC Standard (implementing the CMMC Model created by DoD)
  - Developing CMMC-related Testing and Accreditation Requirements
  - Licensing Training Organizations and Curriculum
  - Licensing Trainers
  - Licensing Certified 3rd Party Assessment Organizations ("C3PAOs")
  - Licensing Assessors
  - Issuing Certificates to Organizations Seeking Certification

How is the CMMC-AB Organized?

- Registered as a non-stock corporation in Maryland.
- Currently the CMMC-AB Consists of a volunteer Board of Directors
  - The current directors represent small and large organizations from a wide range of stakeholder segments;
  - Directors serve as individuals and not representatives of their parent organizations;
  - Individuals seeking to serve as individual assessors or affiliated with an aspiring C3PAO are not allowed to serve as directors;
  - Individuals serving on the board are subject to a strict Conflict of Interest Policy that requires disclosure and recusal on topics where the member may be an interested party.

How is the CMMC-AB Funded?

- The CMMC-AB does not expect to receive any funding from DoD.
- CMMC-AB is exploring several funding options.
- Application for recognition as a nonprofit entity under IRS Code section 501(c)(3) is still pending.
- Organizations or other entities with grant/lending opportunities should reach out to CMMC-AB Board of Directors Chairman Ty Schieber.

Where is the CMMC-AB Located?

- Short term: Headquarters within 50 miles of the Pentagon (most likely Maryland or Virginia).
- Long term: CMMC-AB expects to have at least a nation-wide footprint to meet industry's needs.
  - The intent is to ensure cost effective positioning of CMMC-AB resources to accomplish the objectives of CMMC and ensure appropriate distribution of opportunity and economic impact in communities across the nation.

Will the CMMC-AB Conduct Assessments?

- No. Assessments will be conducted by independent, licensed Assessors.
- C3PAOs will vouch for the Assessor's method of conducting assessments.
- Assessments will be subject to CMMC-AB's QA process before Certification is issued by the CMMC-AB.

How can my Organization get CMMC Certified?

- **Right now, you can't.**
- DoD released CMMC Version 1.0 on 31-JAN-2020.
- CMMC-AB is working on defining the standard, as well as the infrastructure to support licensing of C3PAOs and Assessors and certifying contractors and other organizations.
- **There are no CMMC-AB approved C3PAOs or Assessors at this time.**
- That does not, however, mean that your organization should not begin preparing for CMMC.

How can my Organization Prepare for CMMC?

- Use NIST 800-171 and CMMC Version 1.0 as a basis for evaluation.
  - The exact requirements to meet any given CMMC control have not been drawn and thus all formal assessments will have to wait until later.
- Begin creating associated documentation. This is advantageous even if the organization only expects to stay at Level 1.
- Visit https://www.CMMC-AB.org and sign up for the mailing list. All major changes will be announced via the website and mailing list.
- Exciting announcements are in the works – be sure to register!

How can my Organization Become a C3PAO and how can I become an Assessor?

- Right now, you can't.
- Sign up for the mailing list, and as soon as details are finalized they will be announced via the website and mailing list.
- Important note: C3PAOs and Assessors will not be permitted to Assess organizations to which they have provided consulting services.

How can I/my Organization get Involved with the CMMC-AB?

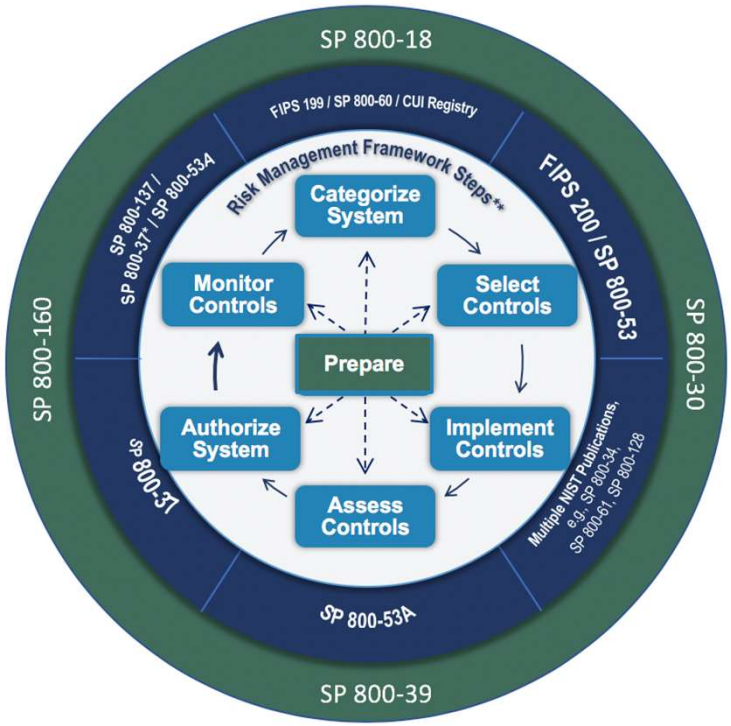
- The CMMC-AB will be creating Industry Working Groups to advise the CMMC-AB Board of Directors.
- Industry, academia, and government participation is welcome and encouraged.
- Currently no Working Groups have been created, but sign up for the newsletter if you are interested in participating as Working Groups will likely be formed soon.

Other Contract Requirements and Resources

Fathom Cyber
Defensible Cybersecurity Strategists

NIST SP 800-37 (Risk Management Framework)

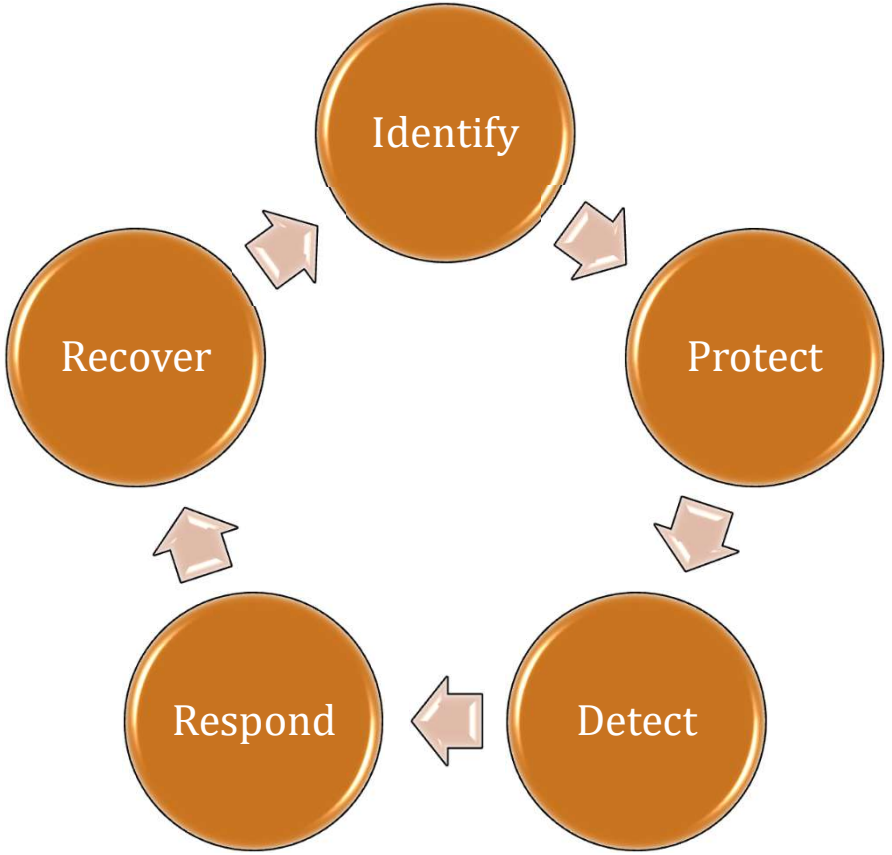
- The Risk Management Framework (RMF) is a set of criteria that dictate how U.S. government IT systems must be architected, secured, and monitored.
  - Originally developed by DOD, the RMF was adopted by the rest of the federal government in 2010
- RMF is a process to architect and engineer a data security process for new IT systems:
  - Step 1: Categorize Information System
  - Step 2: Select Security Controls
  - Step 3: Implement Security Controls
  - Step 4: Assess Security Controls
  - Step 5: Authorize Information System
  - Step 6: Monitor Security Controls
- In addition to the primary document (SP 800-37), the RMF uses supplemental documents SP 800-30, SP 800-39, SP 800-53, SP 800-53A, and SP 800-137



Fathom Cyber
Defensible Cybersecurity Strategists

NIST Cybersecurity Framework

- NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF) is a set of **"optional"** standards, best practices, and recommendations for improving cybersecurity at the organizational level—
  - No mandatory security controls.
  - Mandatory for federal agencies.
  - Heavily adopted commercially.
- CSF features 5 functions used to organize cybersecurity to form a top-level approach to securing systems and responding to threats.
- CSF has 4 tiers of implementation; but not considered "maturity levels."



Fathom Cyber
Defensible Cybersecurity Strategists

NIST SP 800-171 - Overview

- NIST Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations".
- Defines how to safeguard and distribute controlled unclassified information (CUI) on government contractor information systems.
- Contains 14 categories of security controls divided into *Basic Security Requirements* & *Derived Security Requirements.*
- Incorporated into DoD contracts and required for all suppliers, including those supplying commercial items (but not commercial-off-the-shelf items) (DFARS 252.204-7012).
- Contractors may limit the scope of the CUI security requirements to particular systems or network components.

NIST SP 800-171 – Security Control Families

Fathom Cyber
Defensible Cybersecurity Strategists

New Developments [Proposed NIST SP 800-172]

- In June 2019, NIST released SP 800-172, which includes 33 enhanced CUI requirements for "critical systems" and "high value assets".
- The focus of these new requirements is on organizations that are likely targets of advanced persistent threat (APT) attacks.
- "Critical systems" and high value assets" are not defined in 800-172.
- No criteria questions to help determine what qualifies as a critical system or high value asset.
- Unclear how a contractor will be notified by an agency that it is operating a critical program or high value asset.
- Unclear whether an agency can designate a critical system or high value asset after contract award and during contract performance.

NIST SP 800-53 & FISMA

- FISMA refers collectively to:
  - Federal Information Security Management Act of 2002
  - Federal Information Security Modernization Act of 2014
- FISMA ranks systems as “Low,” “Moderate,” and “High”
- Compliance required where the federal agency has made the determinations under FIPS 199 & FIPS 200.
- FISMA is synonymous with NIST SP 800-53:
  - NIST SP 800-53 recommends security controls for federal information systems and organizations and documents security controls for all federal information systems, except those designed for national security
- NIST SP 800-53 is currently at Revision 4, but NIST has issued Draft Revision 5 for public comment.

Federal Information Processing Standards

- The Federal Information Processing Standards (FIPS) are a set of standards published by the National Institute of Standards and Technology (NIST).
- FIPS describe document processing, encryption algorithms, and other IT standards for use within civilian government agencies and by contractors to comply with FISMA.
- FIPS 140-2: Specifies the security requirements for cryptographic modules protecting sensitive information.
- FIPS 199: Categorizes the risk of a system according to “confidentiality,” “integrity,” and “availability”; then divides the systems into ”high,” “moderate,” and “low” impact systems based on their impact on individuals and organizations.
- FIPS 200: Specifies the minimum security requirements (in 17 areas) for civilian federal information systems.

FedRAMP

- Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach to security assessment, authorization, and continuous monitoring (ConMon) for cloud service offerings (CSOs).
- FedRAMP uses the NIST Federal Information Processing Standards (FIPS) and FISMA 800-53 defined control standards.
- FedRAMP ranks CSOs at "LI SaaS" (38 controls), "Low" (125 controls), "Moderate" (325 controls), and "High" (421 controls).
- There are two ways to authorize a CSO under FedRAMP:
  - Joint Authorization Board (JAB) provisional authorization to operate (P-ATO), and
  - Through individual agencies
- Consultants help get CSOs "FedRAMP Ready," while Third Party Assessment Organizations (3PAO) perform the security assessments of CSOs.
- The federal agency consuming the service still has final responsibility for final authority to operate.

DoD Cloud Computing Security Requirements

- The Defense Information Systems Agency (DISA) developed the *DOD Cloud Computing Security Requirements Guide* (*SRG*)
  - Defines the baseline security requirements for cloud service providers (CSPs) that host DOD information, systems, and applications, and for DOD's use of cloud services.
  - Maps to the DOD Risk Management Framework, NIST SP 800-37, and NIST SP 800-53, and can leverage FedRAMP.
  - Leverages FedRAMP "Moderate" (325 controls + additional controls for IL4, IL5, and IL6 – up to ~478 controls).
  - Provides standard assessment and authorization process for CSPs to obtain a DOD Provisional Authorization (PA), which allows DOD components to leverage the CSP's environment without individualized assessment and authorization.
  - Rates risk by Impact Level (IL) (e.g., IL4, IL5).