April 21, 2022

Looking Ahead…

Cybersecurity Maturity Model Certification (CMMC) Regulatory Introduction and Roadmap

Jerry Leishman (EVP/National Regulatory Compliance Director)
Jerry.leishman@cortacgroup.com

CORTAC GROUP

PUBLIC CONTRACTING INSTITUTE

INTRODUCTIONS

Jerry.leishman@cortacgroup.com
206-484-9936

Jerry Leishman

EVP/National Security & Compliance Director

In Process

Jerry is a trusted advisor and advocate for in-house counsel, compliance officers and senior leadership to ensure they can effectively navigate complex regulatory and contractual risks and obligations. He leads CORTAC Group Regulated security & compliance practice supporting Defense suppliers of all sizes and cybersecurity postures.

He is an expert at risk-based approaches embracing right-size outcomes that are cost-optimized to meet an organizations required security and compliance requirements. He is closely aligned with industry and technology leaders including Microsoft, AWS, and Exostar in delivering world- class solutions.

Jerry is active nationally on the CMMC AB Standards Workgroup, a Provisional CMMC Assessor & Registered Practitioner (RP). Jerry speaks nationally on DFARS and CMMC impacts, and partners with private/public organizations to increase the Pacific Northwest Defense and Aerospace manufacturer awareness.

CMMC CONSORTIUM

CORTAC GROUP

SUMMIT7

Quzara.com Cloud. Security. Analytics.

Microsoft

Founding Member of the CMMC Consortium - partnering with Microsoft, Summit 7, and Quzara brings integrated solutions to small, medium, and large defense, aerospace and commercial suppliers

AGENDA

National Security & Defense Landscape

CMMC 2.0 Overview

Defense Industrial Base (DIB) Impact

CMMC Journey

Key Take Aways

NATIONAL SECURITY & DEFENSE LANDSCAPE

DEFENSE & AEROSPACE

"The United States' strategic competitors and adversaries are conducting cyber-enabled campaigns to ***erode U.S. military advantages, threaten our infrastructure, and reduce our economic prosperity.***

This constitutes one of our most critical national security concerns."

Department of Defense

NATIONAL SECURITY & DEFENSE LANDSCAPE

GLOBAL ORGANIZATIONAL IMPACT

Cyberattacks are the fastest growing crime in the U.S., and they are increasing in size, sophistication and cost.

“Cyber crime may be the greatest threat to every company in the world”

Former IBM Corp.'s Chairman, CEO and President, Ginni Rometty

NATIONAL SECURITY & DEFENSE LANDSCAPE

HAPPENING TODAY

Lockheed Martin, General Dynamics, Boeing, Tesla, and SpaceX are among dozens of companies named as victims of compromised data, accessed through the hacking of precision parts manufacturer Visser Precision LLC, a Colorado-based aerospace, automotive and industrial parts manufacturer.

March 2020

Solar Winds - IT
Colonial Pipeline – Oil & Gas
JBS Meats – Consumer Meat
McDonalds - Consumer

Biden Executive Order - Federal

WE SHARE THE COST AND BURDEN OF DEFENDING FREEDOM

$1 TRILLION

Annual Global Supply Chain Exfiltration & Leakage*

300K+ ENTITIES

Global Defense, Aerospace, University, and R&D Supply Chain Organizations*

80% FLOW DOWN

Percent of DoD Intellectual Property on Non-DoD Supplier & University Networks*

AVERAGE OF 314 DAYS FROM DATA BREACH TO CONTAINMENT

Average of 7 months to identify a breach, and another 4 months to contain it.

"The United States' strategic competitors and adversaries are conducting cyber-enabled campaigns to erode U.S. military advantages, threaten our infrastructure, and reduce our economic prosperity.

This constitutes one of our most critical national security concerns."

Department of Defense

FEDERAL GOVERNMENT RESPONSE

Current law today for DoD suppliers with DFARS flow downs

ITAR/EARS

1976

- Restrict and control the export of defense and military related technologies and information
- Safeguard U.S. national security and further U.S. foreign policy objectives

DFARS 252.204-7012, NIST (SP) 800 – 171

2018

- Protect controlled unclassified Information (CUI) in non-federal systems and organizations
- Mandatory System Security Plan (SSP) & Plan, Action & Milestone (POA&M), & Cyber Incident Reporting
- Self attestation of 110 cyber controls

DFARS 7012 Interim Rule 252.204-7019, 7020, 7021

2020

- Must report NIST SP 800-171 compliance to DoD SPRS for future contract awards
- Contractor must provide government physical access to facilities, systems, and personnel
- Cybersecurity Maturity Model Certification (CMMC) certificate for DoD contracting

CMMC 2.0

2023+

- Unified cyber security standard (DFARS+) with multiple levels
- Incorporate CMMC 7021 into Federal CFR 32 and CFR 48 (make it Federal law)
- Primes are responsible for all down-level supplier CMMC compliance
- Supplier CMMC certification is 3rd party audit and **“go/no-go decision”**

“In order to win a contract or successfully rebid on a contract, you will need to pass the CMMC audit.”

Ellen Lord

Under Secretary of Defense for Acquisition and Sustainment (A&S)

DoD CMMC GOALS

- **Protect Controlled Unclassified Information (CUI)**
  - Protect nonfederal organization's internal systems processing, storing, or transmitting CUI
  - Standardize and provide clarity on cybersecurity regulatory, policy, and contracting requirements;
  - Focus on the most advanced cybersecurity standards and third-party assessment requirements on companies supporting the highest priority programs;
- **Increase Accountability**
  - Increase DoD oversight of professional and ethical standards in the assessment ecosystem.
  - Ensure accountability for companies to implement cybersecurity standards while minimizing barriers to compliance with DoD requirements;
- **Increase Public Trust**
  - Instill a collaborative culture of cybersecurity and cyber resilience; and
  - Enhance public trust in the CMMC ecosystem, while increasing overall ease of execution.

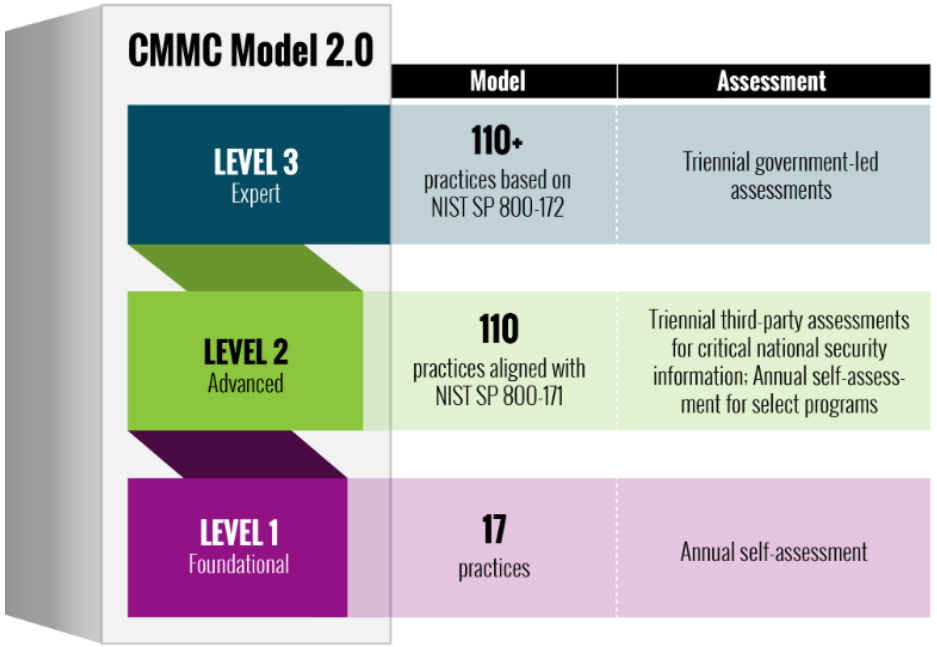
"**CMMC 2.0** will dramatically strengthen the cybersecurity of the defense industrial base, by establishing a more collaborative relationship with industry, these updates will support businesses in adopting the practices they need to thwart cyber threats while minimizing barriers to compliance with DoD requirements."

Jesse Salazar, Deputy Assistant Secretary of Defense for Industrial Policy.

CMMC 2.0 OVERVIEW

CMMC 2.0 is a unified cybersecurity standard for future DoD acquisitions built on FAR/NIST 800-171

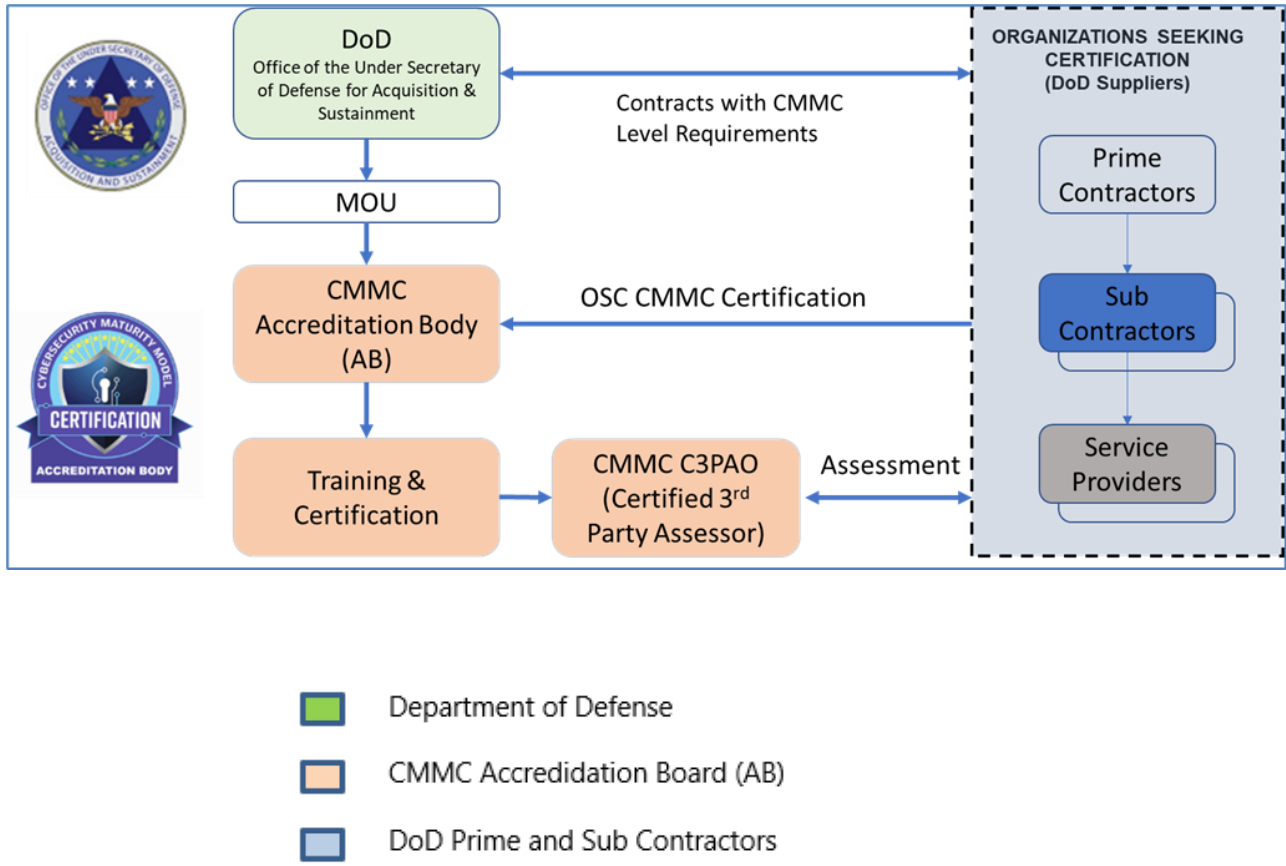
- DFARS 7012 Interim Rule (based on NIST 800-171) – Effective November 30, 2020 **(Law of land today!)**
- Protection of DoD information across supply chain
  - **Federal contract information** (FCI) means information, not intended for public release, that is provided by or generated for the Government under a contract
  - **Controlled Unclassified Information** (CUI) means unclassified government information marked and classified as "CUI" for purposes of requiring special handling (Store, Transmit, Create, and/or Process) under United States Department of Defense ("DoD") regulations.
  - **International Traffic in Arms Regulations** (ITAR) contains a United States Munitions List (USML) of restricted articles and services per U.S. State Department's Directorate of Defense Trade Controls (DDTC).
- Requires annual Self-Attestation or triennial 3rd Party assessment certification prior to contract award.
- Primes are responsible for down-level supplier CMMC compliance
- **Proposed CMMC 2.0 Rule Making Complete in early 2023**



- **Level 1** is equivalent to all of the safeguarding requirements from FAR Clause 52.204-21. It is focused on protecting FCI for organizations such as landscapers, food service, etc.
- **Level 2** is equivalent to all of the security requirements in NIST SP 800-171 Revision 2. It is focused on protecting CUI and ITAR for organizations such as manufacturers, cloud service providers, etc.
- **Level 3** will be based on a subset of NIST SP 800-172 and more detailed information will be released at a later date. It is focused on protecting higher sensitivity CUI and ITAR.

CMMC ECOSYSTEM

- **DoD** – Responsible for national security and data protection and cybersecurity across the entire Defense supply chain and ensure its resiliency
- **CMMC-AB** - establishes and oversees a qualified, trained, and high-fidelity community of assessors that can deliver consistent and informative assessments to participating organizations against a defined set of controls/best practices within the CMMC Program.
- **Training & Certification** – CMMC AB oversees CMMC education and training services for certified CMMC professionals (CCP) and Certified CMMC Assessor (CCA)
- **C3PAOs** - an organization authorized by the CMMC-AB to conduct and deliver CMMC assessments after entering into a contract with an Organization Seeking Compliance (OSCs).
- **Prime Contractor** - The DoD prime contractor is the private companies that DoD directly contracts to provide products or services.
- **Sub-Contractors** - A subcontractor is an individual or a business that signs a contract to perform part or all of the obligations of a DoD prime or sub-contractor (sub-levels 1 to 8) contract. These includes precision manufacturers, product assembly, etc.
- **Service Providers/Vendors** - A Service Provider/vendor includes entities with whom the institution has a contract or conducts commerce. These include MSP, MSSP, Consultants, Facilities vendors, Janitorial, etc.



CMMC MODEL FRAMEWORK

Framework

- The CMMC model measures the implementation of the NIST SP 800-171 Rev 2 framework including:
    - 14 Domain Families
    - 110 Practices (security controls)
    - 320 Control Objectives (requirements)

Model Hierarchy

- Each **Domain** will have one to many applicable **Practices** based on level
- Each **Practice** will have one to many applicable **Assessment Objectives** based on level
- Each CMMC level **inherits** the requirements from all lower levels

Assessment Procedure Methods

- An assessment procedure consists of an assessment *objective* and a set of potential assessment *methods* and assessment *objects* that can be used to conduct the assessment

- The application of each method is described in terms of the attributes of *depth* and *coverage*, progressing from *basic* to *focused* to *comprehensive*
    - Examine
    - Interview
    - Test

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

DOMAIN: ACCESS CONTROL (AC)

PRACTICES		
Level 1	**Level 2**	**Level 3**
AC.1.001 **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.2.016 **AC.L2-3.1.3** *Control CUI Flow* Control the flow of CUI in accordance with approved authorizations. • NIST SP 800-171 Rev 2 3.1.3	
AC.1.002 **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.3.017 **AC.L2-3.1.4** *Separation of Duties* Separate the duties of individuals to reduce the risk of malevolent activity without collusion. • NIST SP 800-171 Rev 2 3.1.4	
AC.1.003 **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	AC.2.007 **AC.L2-3.1.5** *Least Privilege* Employ the principle of least privilege, including for specific security functions and privileged accounts. • NIST SP 800-171 Rev 2 3.1.5	

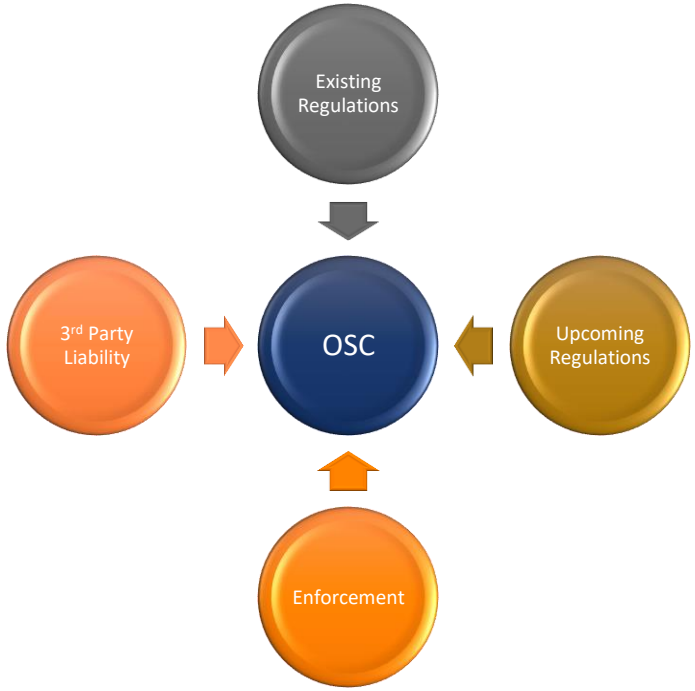
3.1 ACCESS CONTROL

3.1.1	**SECURITY REQUIREMENT** Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.1[a]	*authorized users are identified.*
	3.1.1[b]	*processes acting on behalf of authorized users are identified.*
	3.1.1[c]	*devices (and other systems) authorized to connect to the system are identified.*
	3.1.1[d]	*system access is limited to authorized users.*
	3.1.1[e]	*system access is limited to processes acting on behalf of authorized users.*
	3.1.1[f]	*system access is limited to authorized devices (including other systems).*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities]. Test: [*SELECT FROM:* Organizational processes for managing system accounts; mechanisms for implementing account management].	

CURRENT DFARS/CMMC STATUS

- **DFARS 7012 Interim Rule (In Effect today)**
  - **Effective November 30, 2020**, requiring NIST 800-171 self assessment score reporting to DoD SPRS system (Note: applies to Defense Suppliers with DFARS flow down clauses)
  - DIBCAC will be verifying SPRS scores starting **May 2022**

- **CMMC 2.0 Announced – May 4, 2021**
  - Simplifying the CMMC standard and providing additional clarity on cybersecurity regulatory, policy, and contracting requirements;
  - Focusing the most advanced cybersecurity standards and third-party assessment requirements on companies supporting the highest priority programs
  - Increasing Department oversight of professional and ethical standards in the assessment ecosystem
  - Ensure accountability for companies to implement cybersecurity standards while minimizing barriers to compliance with DoD requirements
  - Instill a collaborative culture of cybersecurity and cyber resilience
  - Enhance public trust in the CMMC ecosystem, while increasing overall ease of execution.



- **CMMC Federal Rule Making (targeted May 2023)**
  - CMMC 2.0 will be implemented through the rulemaking process both in Part 32 of the Code of Federal Regulations (C.F.R.) as well as in the Defense Federal Acquisition Regulation Supplement (DFARS) in Part 48 of the C.F.R. **Expected to be completed May 2023.**
  - Companies will be required to comply once the forthcoming rules go into effect. Both rules will have a public comment period.

- **Utilized Frameworks (FAR & NIST)**
  - CMMC 2.00 model based on FAR (Level 1) & NIST SP 800-171 (Level 2)
    - Level 1 – FAR Self-Attestation and SPRS score
    - Level 2 – NIST SP 800-171 3rd Party Audit

CMMC BREADTH – WHO IS IMPACTED?

US DoD

Supply chain for the US Department of Defense

Commercial

Commercial companies manufacturing and providing services

350K

350K companies - 80% are small/medium

Under constant attack

Risk to national security

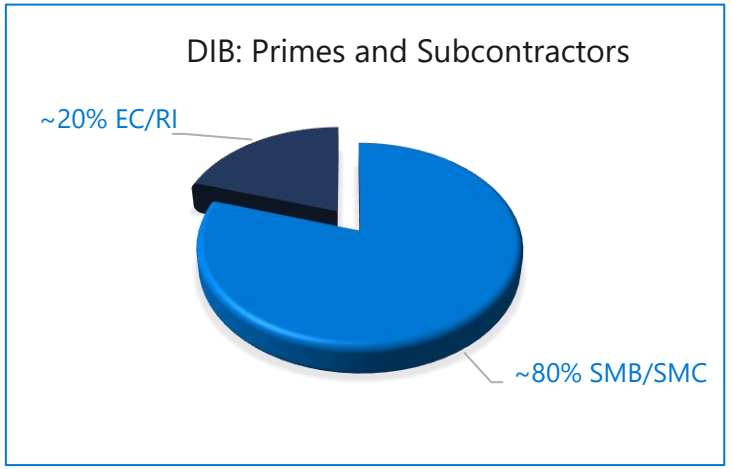
$5.1T at risk over next 5 years[1]

[1] "Ninth Annual Cost of Cybercrime Study" by Accenture in 2019

CMMC DEPTH - DEFENSE INDUSTRIAL BASE (DIB)

The Defense Industrial Base (DIB) enables research and development, design, production, delivery, & maintenance of military weapons systems, subsystems, and parts/components that are essential to mobilize, deploy, and sustain U.S. military operations, including:

1. Complex platforms unique to the military
    - E.g., aircraft carriers, amphibious assault vehicles
2. Highly specialized services
    - E.g., satellite launch systems, missile defense systems
3. Commercial products
    - E.g., laptop computers and semiconductors
4. Routine services
    - E.g., systems maintenance, information technology support



Approximately 80% of DIB companies are small and medium businesses (SMBs)

INDUSTRY CHALLENGES & GAPS

Increasing Laws, Regulations, & Expectations

- **Significant Increases** - Defense and Aerospace supply chain legal and regulatory governmental requirements (e.g., ITAR, DFARS, EAR, FAR, CMMC, FedRAMP, etc.)
- **New Federal Incident Response Reporting –** Multiple federal government organization and congress have recently implemented Cybersecurity Incident Response requirements (72-hour reporting)
- **Limited Investment-** Majority of contractors have not sufficiently invested & implemented NIST 800-171 (Government believes they have)
- **Upcoming 3rd Party Audits** - In 2023, a 3rd Party assessment for Cybersecurity Maturity Model Certification (CMMC) Level 2/3 will be required

Significant Penalties for Non-Compliance

- **Legal & Personal Accountability**
  - Consent Decrees, Civil Penalties, Criminal Penalties, & Disbarment
  - Increasing False Claim Act (FCA) resources and enforcement currently underway
- **Business and Contract Loss**
  - Disqualification for non-compliance of DFARS 7012, resulting in loss of current and future business
  - DIBCAC verifications of SPRS scores will begin May 2022
  - CMMC 2.0 will require 3rd party audits by C3PAOs
- **Brand Impact**
  - Breaches increase organizational loss of current and future business and being an ongoing entity
  - Reputation impacts, lawsuits, stock price declines, CEO resignations, etc.

INDUSTRY CHALLENGES & GAPS

Organizations Not Prepared

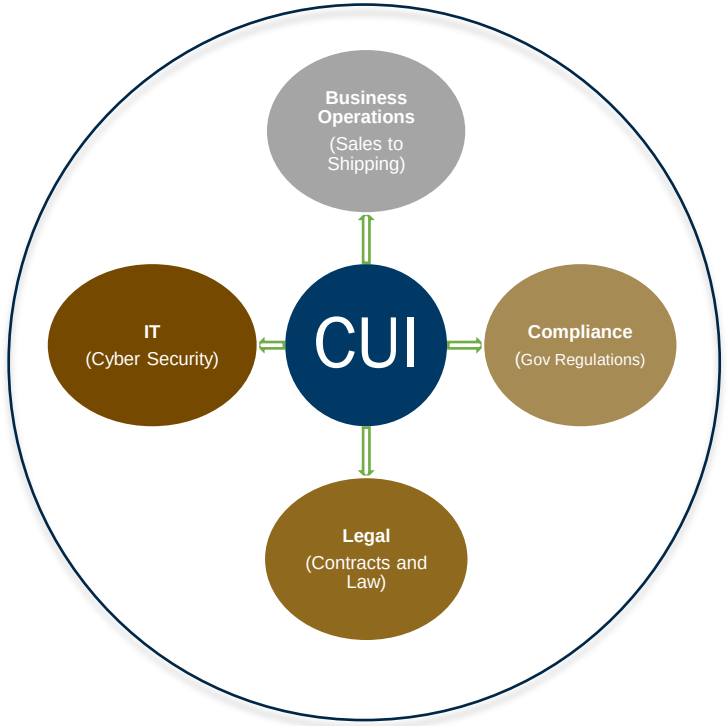
- **Leadership Understanding**
  - Complex and changing legal and regulatory requirements (e.g., CMMC)
  - Uncertain personal & enterprise obligations and risks
  - Lack of executive alignment across IT, Legal, business, & compliance
  - Unclear risk optimization roadmap and cost investment strategy

- **Unknown Compliance Gaps & Risks**
  - Unified security & compliance framework for enterprise (multiple regimes/CMMC)
  - CUI management controls across physical and digital enterprise
  - Consolidated processes, documentation, tools & training
  - Lack of required enterprise security & compliance documentation

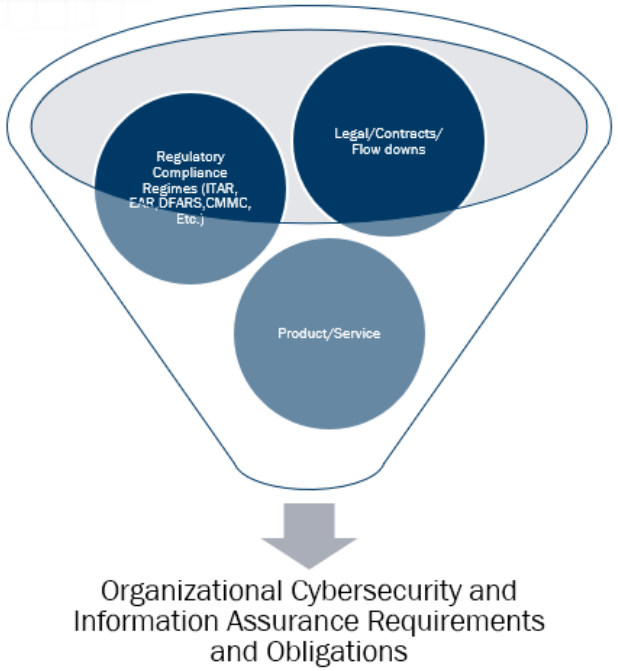
- **Required Skills, Capabilities, & Funding**
  - Expertise to identify or mitigate risks of non-compliance and cybersecurity
  - Responsibility for supply chain management & information sharing
  - Lack of business prioritization & budget

"Majority of contractors have not implemented NIST 800-171 (Cyber DFARS) within their information systems"

Office of the Under Secretary of Defense for Acquisition and Sustainment



WHAT IS NEEDED?
SYSTEMATIC APPROACH



Identify Business Obligations & Risks

Executives must align on organizational cybersecurity and information assurance requirements, obligations and business risks to make strategic decisions and investments

- **Identify information subject to** U.S. Government legal, contractual, and regulatory requirements mandating information protection and control
- **Identify regulated and sensitive information** flows, transformations, identification, sharing and management required to support business activities
- **Evaluate** governance, risk management, process, systems, operational and technical sufficiency to minimize legal, contractual and regulatory risks

Identify Variances & Solutions

Operational leaders need a detailed understanding of their regulatory compliance gaps and risks, enabling mitigation roadmaps and solutions

- Identify “current state” variances - data management, documentation, and operations
- Develop gap and risk mitigation recommendations and cost estimates
- Define risk-based approach and cost optimized roadmap
- Create compliance documentation and artifacts

Execute Compliance Program Adherence

Compliance officers require a on-going risk prioritized mitigation roadmap to ensure executive visibility, drive risk/cost optimized mitigations & implementations.

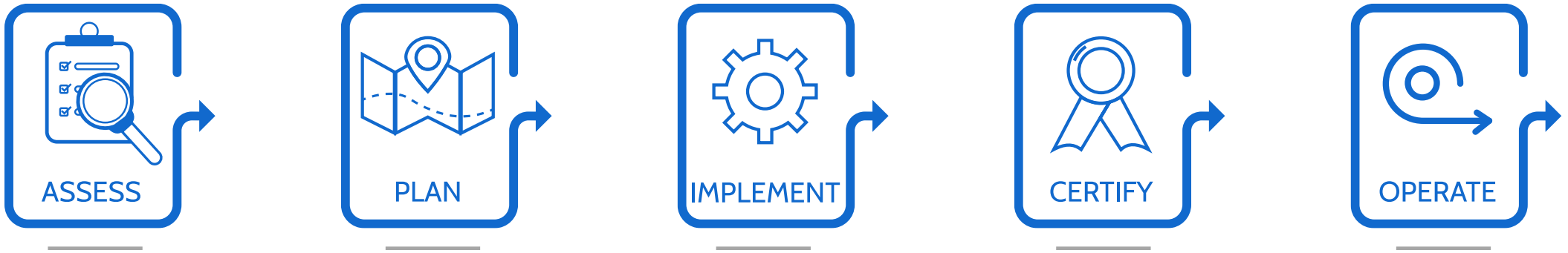
- Enable compliance program management office to drive mitigation and certification
- Oversee compliance mitigation risk and cost optimization roadmap
- Provide detailed compliance requirements, verification and solution implementation support
- Maintain regulatory and compliance documentation

CMMC 2.0 JOURNEY BREAKDOWN

Plan

Implement

Operate



Prepare for DFARS/CMMC Journey

- Understand Obligations
- Define FCI/CUI boundary
- Identify Baseline Gaps & Risks
- Develop Roadmap

Identify Gap Mitigation Solutions

- Define solution selection criteria
- Identify “right sized” architecture & solutions
- Establish Shared Resource Responsibilities
- Develop Implementation plan, costs, and timeline

Implement Solutions & Institutionalize

- Implement Technical Solutions & Configurations
- Migrate FCI/CUI information
- Implement Compliance Program
- Documentation (Policy, Procedure, SSP, POA&M, etc.)
- Security Monitoring

Orchestrate Assessment

- Prepare and Package Evidence
- Identify & Schedule C3PAO Assessor
- Pre-Assessment
- Perform Assessment

Maintain Ongoing Compliance

- Compliance Resiliency
- Change Management
- Documentation Maintenance
- Incident Response
- Reporting and Audit Support

YOUR OPTIONS

Yes, this is going to cost money.

You have four options:

1. Do nothing. Break your contracts. Lose data. Get caught.
2. Fix the security deficiencies and fix things before you receive a CMMC contract.
3. Implement a minimal solution to meet compliance objectives.
4. Secure your data and your business.

YOUR CMMC PATH FORWARD

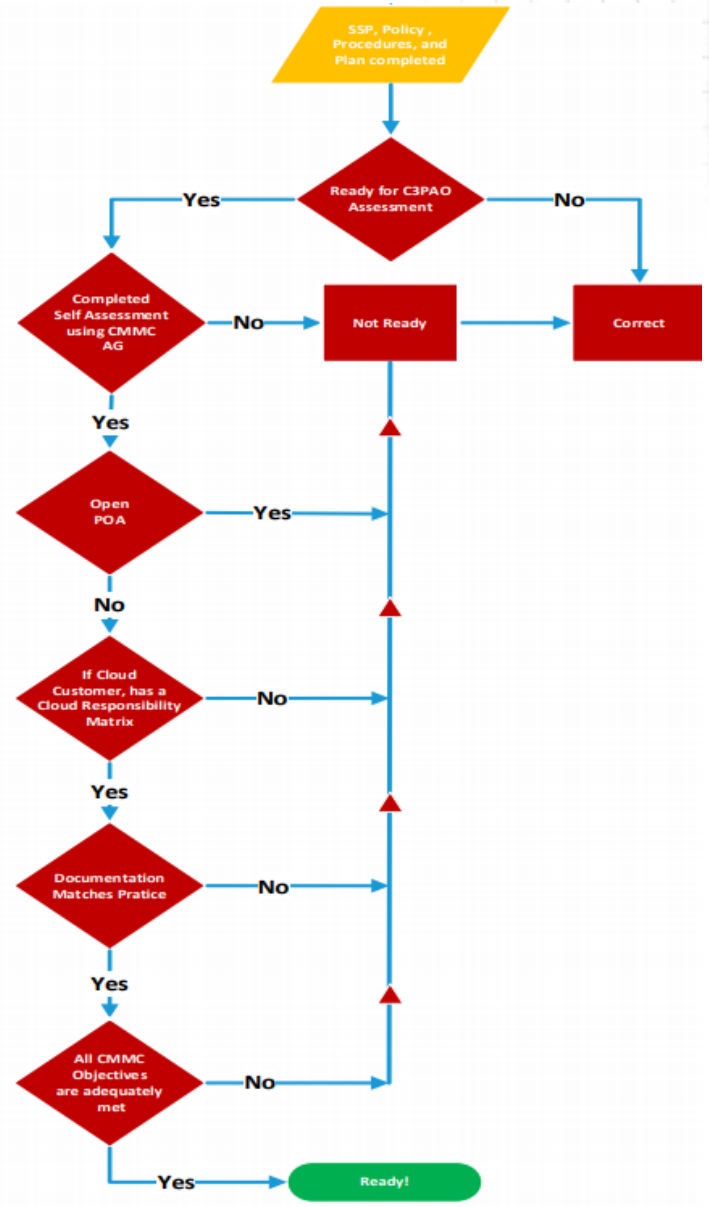
Planning Checklist

- ✓ Leverage a proven guide & navigator **(e.g., consultant)**
- ✓ Fill gaps with an integrated & credible team of suppliers
- ✓ Select “right sized & cost optimized solutions” for organization
- ✓ Identify available Federal, State, or Local Funding
- ✓ Develop your End-to-End process & roadmap
- ✓ Achieve & Maintain your CMMC 2.0 certification
  1. Get Secure & Compliant First
  2. Stay Compliant and Secure for 3 years

Get Started Now – it may take 1 to 3 years to achieve your CMMC 2.0/NIST 800-171 requirements

ARE YOU CMMC "AUDIT READY"?

- **Documentation** - Documented System Security Plan (SSP) & incident response ready & not in "draft"
- **Self Assessment** - Completed NIST 800-171 Self Assessment and reported SPRS scores & plan (Interim DFARS Rule Requirement)
- **Plan of Action & Milestone (POA&M)** – nothing open
- **Policy & Procedures** – are repeatable and adequate to implement each practice and practice objectives are met
- **Cloud** – Cloud Customer Responsibilities Matrix (Inheritance matrix related to SSP, policy, and procedures)
- **BYOD** – explanation in SSP, documented procedures, network diagrams, and documentation on how technical controls are being met
- **Processes** – Processes are documented and performed (Institutionalized)



ORGANIZATIONAL BENEFITS

"DoD ITAR, DFARS & CMMC regulatory & cybersecurity requirements provides a systematic approach to achieve increasing cybersecurity requirements and protecting customer and corporate intellectual property."

- **Increases Leadership Call To Action -** Facilitates Senior leadership understand, alignment, and prioritization of information protection investments
- **Increases Information Protection**
  - **Minimizes Unauthorized Disclosures** - Increased process and practices to protect ITAR & EAR information from being disclosed to unauthorized entities and individuals
  - **Protects Internal Systems**- Incorporates internal system information protection, governance and security to protect ITAR, CUI, FCI and other corporate IP from supply chain exfiltration
  - **Establishes Resilient Compliance Program** - Enforces a systematic compliance program and approach that demonstrates and enhances reasonable due care
- **Reduces Risk of Non-Compliance Penalties** – Reduces risk of non-compliance penalties such as contract loss and disqualification, civil and criminal lawsuits, False Claims Acts, and negative brand impact.
- **Increases Competitive Advantages** – Customer trust and a low-risk security and compliance posture, will gain advantages to win more business.

KEY TAKEAWAYS

- Information Protection is a business Challenge and requirement, Not just an IT issue
  - In-house council & compliance officers are responsible to ensure all regulatory and cybersecurity risk is addressed
- Significant organizational leadership collaboration & alignment will be required
  - Inhouse counsel, compliance officer, CIO, and business product owners own CUI, from Sales to Shipping, and crosses people, process and technology
- Can't fake it till you make it anymore
  - You will have to pay to play to receive DoD contract awards and meet customer contract requirements
- Efficiency and cost optimization will require a systematic enterprise approach
  - instead of whack a mole
- Data Protection shortcuts won't get you there anymore
  - Data enclaves and awkward workflows only increase information leakage and exfiltration risk
- You will need experts to help
  - Most organizations do not have the skills and capabilities to understand and implement solutions to meet regulatory requirements, thus leaving the organization at high risk of non-compliance and penalties
- CMMC, or similar, will become tables stakes to modern business
  - Federal, State, Local, International and Commercial Contracts will adopt CMMC like baseline requirements in their contracts
- Get started now - Non-Compliance Penalties are high & tide is rising
  - Most organizations have a low maturity and a significant amount of work to do to meet upcoming CMMC compliance requirements and certification to keep existing contracts and win new business

Compliant. Secure. Risk Optimized

Contact Information

If you'd like additional information on how CMMC, Regulated Data (ITAR/EAR/NIST), or future DoD acquisition will affect your organization, please reach out directly:

- Jerry Leishman - jerry.leishman@cortacgroup.com (www.cortacgroup.com)

Our goal is to increase your competitive advantages & business capture rate and protect your Enterprise information from adversaries.

THANK YOU!!

We’re on this mission with you

Jerry Leishman

- 1 of 12 members of the National CMMC Accreditation Board Standards Workgroup
- CMMC Level 1-3 Provisional Assessor
- CMMC Registered Practicioner

CORTAC Group is a Registered Provider Organization (RPO) and in process of obtaining C3PAO status

---

CORTAC GROUP

SUMMIT7

Quzara.com
Cloud. Security. Analytics.

Microsoft

Founding Member of the CMMC Consortium - partnering with Microsoft, Summit 7, and Quzara brings integrated solutions to small, medium, and large defense suppliers

---

Microsoft Partner

Cortac Group is an insider and strategic Microsoft Government partner. We participate in internal projects as well as co-sell and deliver right-sized solutions to Defense suppliers.

Trusted Guide, Advisor, Advocate & Therapist

Everyday, we walk with executive leaders and stakeholders at Fortune 100 companies as they secure their organizations and supply chains from nation states, global criminals, and avoid non-compliance penalties.

Our Story

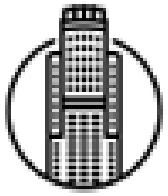
INTRODUCTION TO CORTAC

BY THE NUMBERS

13	79	350+	30+	100+
Years in Business	Clients (21 in the Fortune 500)	Projects Delivered	Countries Serviced	Team Members

OUR OFFICES

Seattle, WA



Los Angeles, CA

Washington DC

KEY CLIENTS

Microsoft

BAE SYSTEMS

Anthem

LOCKHEED MARTIN

SAP Concur

BLUE ORIGIN

amazon web services

BOEING