



CYBER CAPITAL
PARTNERS

SOLVING CMMC FOR SMALL BUSINESS



SPONSORS

**PILIERO
MAZZA**

HARTMAN
EXECUTIVE ADVISORS

RIMSTORM



CyberDI
CMMC | Training | Consulting | Solutions

PH
ProposalHelper
Human Solutions for Business Growth

DHG
DIXON HUGHES GOODMAN LLP

WEBINAR BASICS

01

Due to the large number of participants, **this webinar is set to mute all lines** and disable cameras and video.

02

Today's session will be recorded and posted at www.cybercp.com

03

If you have a technical problem, **please send an email to media@cybercp.com**

04

Please share your thoughts on the presentations during the polling at the event.



AGENDA

2:00-2:05

Welcome & CyberCP

2:05-2:10

Introduction to CMMC

2:10-2:15

CMMC: Legal Ramifications

2:15-2:20

CMMC: Cost Reimbursements

2:20-2:45

Panel Discussion

2:45-2:55

Q&A: All Topics

2:55-3:00

CMMC Concierge

3:00

Evaluation & Close



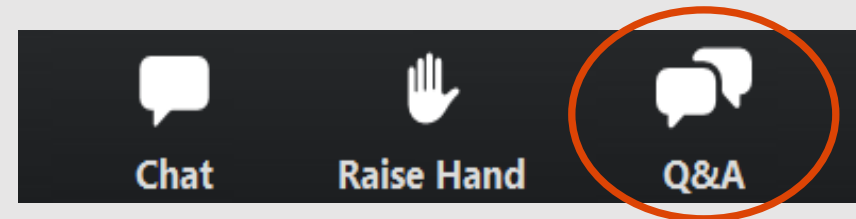
We encourage you to submit questions throughout the presentations

01

Ask questions via the “Q&A” button at the bottom of your screen

02

Type your question into the “Question and Answer” dialog box

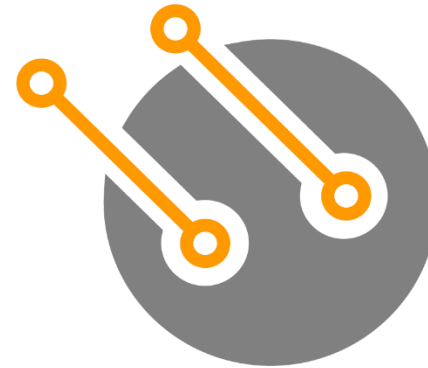


SPONSORS

PILIERO
MAZZA



DHGC
DIXON HUGHES GOODMAN LLP



CyberDI
CMC | Training | Consulting | Solutions

RIMSTORM



ProposalHelper™
Human Solutions for Business Growth

Cyber Capital Partners' Leadership Team



Jason Gayl

Managing Partner

***Corporate
Development***



Fritz Finley

Partner

Operations & Technology



Doug Black

Partner

***Business
Development***



Rich Scigaj, CMA, CM&AA

Partner

***Financial
Management***



Paul Serotkin

Senior Advisor

Federal Funding

A Cadre of Cybersecurity and National Security Industry Experts....

01

Strategic Partnerships

- Teaming Arrangements
- Technology Licensing
- Reseller Arrangements
- New Markets

02

Growth Advisory

- Growth Strategies
- Revenue Pursuit & Capture
- Capabilities Development
- Mergers & Acquisitions

03

Operational Maturity

- Corporate Governance
- Business Process Improvement
- Margin Improvement



CYBER CAPITAL
PARTNERS

SOLVING CMMC FOR SMALL BUSINESS



Introduction to CMMC



Matthew Condly – CEO

CMMC Provisional Assessor (1st Class)

- 25 years' experience in protecting vital information assets, strategic planning



Booz | Allen | Hamilton



DISCOVER



Decorated Career in Advancing US National Security & Compliance

- Harvard University, Certificate in Cybersecurity Risk Management
- Certified Anti-Money Laundering (CAMS), JPMorgan Chase & Discover Card
- Booz Allen Hamilton – 9 years, Counterintelligence & Targeting
- USMC Intelligence Analyst – 8 years 26th MEU & OEF
- College of Charleston (BA), University of Cambridge (MBA)



Experience You Can Count On

Full-service CMMC preparation & assessment company focused on solutions for small and midsize government contractors

Services:

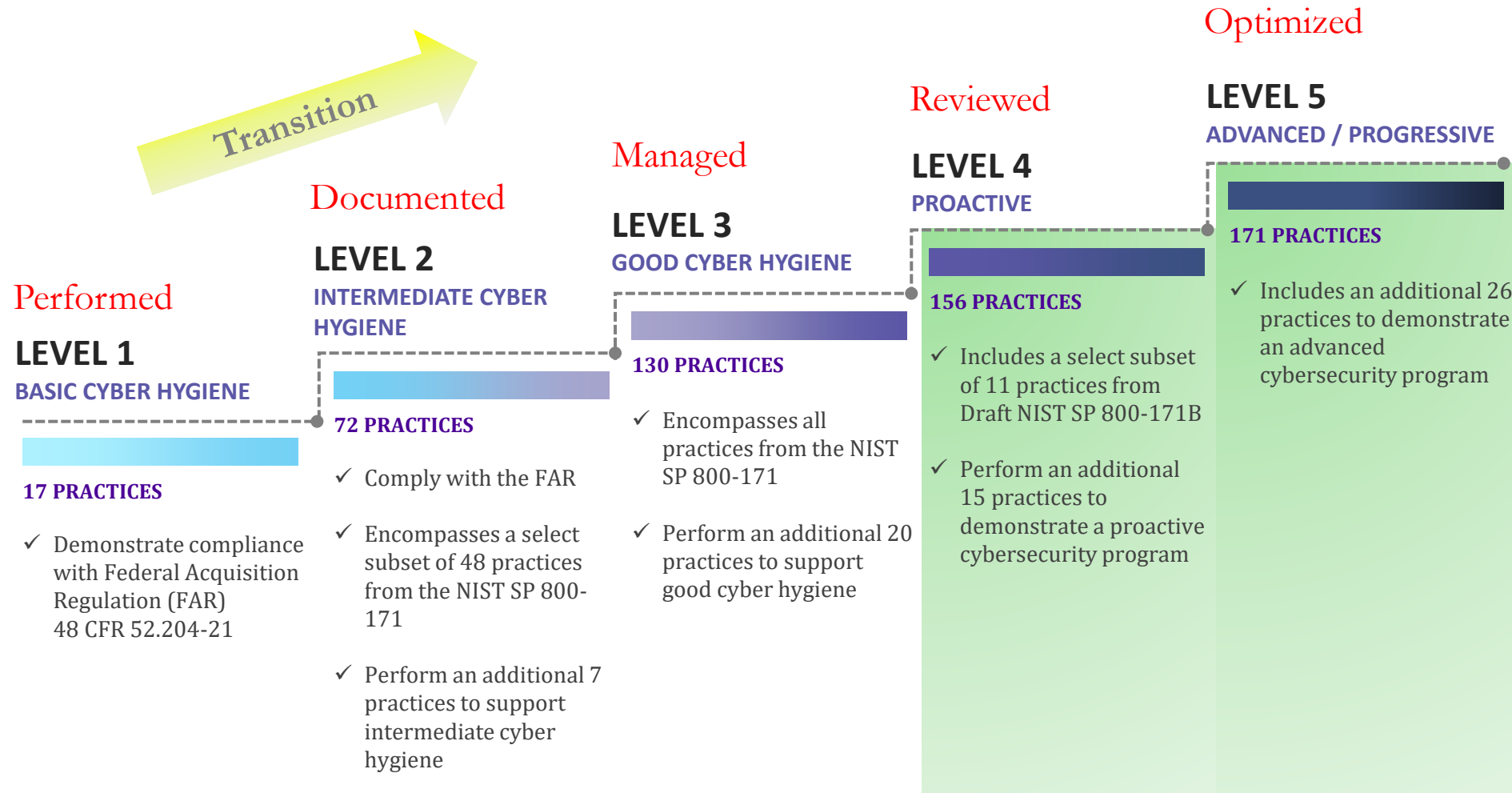
- Pre-assessment readiness review services
- Full CMMC Assessments as a CMMC Accreditation Body (AB) authorized and trained Provisional Assessor (PA).

Manage a network of cybersecurity experts and companies that offer a suite of quality products that will help you get through the CMMC process smoothly.

Interim Rule

- New DFARS 252-204-7020 applies CMMC to DoD contractors and subs
 - Receiving, storing, creating FCI/CUI
 - Effective Nov 30, 2020
- New DFARS 252-204-7021 requires CMMC 3rd party assessment (3 years)
 - Pathfinder Program - identify the first 15 contracts to include the CMMC language
 - Sub-contractor flow down from those contracts is estimated at approximately 1,500
- CMMC Assessment – 5 year roll out
 - Estimated DoD contractors approximately 300,000
 - Estimated that 75-80% will only require maturity level 1 certification
 - ✓ ML1 = 17 performed practices – all encompassed by NIST 800-171 already

Maturity Model Levels



CMMC Domains

ML-1

17

Access Control (AC) - 4/10/8	Incident Response (IR) - 0/5/2	Risk Management (RM) - 0/3/3
Asset Management (AM) - 0/0/1	Maintenance (MA) - 0/4/2	Security Assessment (CA) - 0/3/2
Awareness Training (AT) - 0/2/0	Media Protection (MP) - 1/3/4	Situational Awareness (SA) - 0/1/0
Audit and Accountability (AU) - 0/4/7	Personnel Security (PS) - 0/2/0	System and Communication (SC) - 2/2/15
Configuration Management (CM) - 0/6/3	Physical Protection (PE) - 4/1/1	System and Information Integrity (SI) - 4/3/3
Identification and Authentication (IA) - 2/5/4	Recovery (RE) - 0/2/1	

CMMC Domains

ML-2

55

<p>Access Control (AC) - 4/10/8</p>	<p>Incident Response (IR) - 0/5/2</p>	<p>Risk Management (RM) - 0/3/3</p>
<p>Asset Management (AM) - 0/0/1</p>	<p>Maintenance (MA) - 0/4/2</p>	<p>Security Assessment (CA) - 0/3/2</p>
<p>Awareness Training (AT) - 0/2/0</p>	<p>Media Protection (MP) - 1/3/4</p>	<p>Situational Awareness (SA) - 0/1/0</p>
<p>Audit and Accountability (AU) - 0/4/7</p>	<p>Personnel Security (PS) - 0/2/0</p>	<p>System and Communication (SC) - 2/2/15</p>
<p>Configuration Management (CM) - 0/6/3</p>	<p>Physical Protection (PE) - 4/1/1</p>	<p>System and Information Integrity (SI) - 4/3/3</p>
<p>Identification and Authentication (IA) - 2/5/4</p>	<p>Recovery (RE) - 0/2/1</p>	

CMMC Domains

ML-2

Carry over

Access Control
(AC) - 4/10/8

Incident Response
(IR) - 0/5/2

Risk Management
(RM) - 0/3/3

Asset Management
(AM) - 0/0/1

Maintenance
(MA) - 0/4/2

Security Assessment
(CA) - 0/3/2

Awareness Training
(AT) - 0/2/0

Media Protection
(MP) - 1/3/4

Situational Awareness
(SA) - 0/1/0

Audit and Accountability
(AU) - 0/4/7

Personnel Security
(PS) - 0/2/0

System and Communication
(SC) - 2/2/15

ML-3

Configuration Management
(CM) - 0/6/3

Physical Protection
(PE) - 4/1/1

System and Information Integrity
(SI) - 4/3/3

58

Identification and Authentication
(IA) - 2/5/4

Recovery
(RE) - 0/2/1

CMMC WORKFLOW

SELF-ASSESSMENT

REMEDiation

GAP ANALYSIS

ASSET INVENTORY
IDENTIFICATION

DOCUMENTATION &
TRAINING

EVIDENCE OF DATA
& REMEDIATION

FORMAL
ASSESSMENT

CERTIFICATION

Repeat





CYBER CAPITAL
PARTNERS

SOLVING CMMC FOR SMALL BUSINESS



CMMC: Legal Ramifications



David Shafer
Attorney
PilieroMazza PLLC
Cybersecurity & Data Privacy
410.500.5551
dshafer@pilieromazza.com

PILIERO
MAZZA

CMMC Compliance Considerations for Small Businesses

Dave Shafer, Attorney, Cybersecurity & Data Privacy, PilieroMazza PLLC

December 15, 2020

Disclaimer

This communication does not provide legal advice, nor does it create an attorney-client relationship with you or any other reader. If you require legal guidance in any specific situation, you should engage a qualified lawyer for that purpose. Prior results do not guarantee a similar outcome.

Attorney Advertising

It is possible that under the laws, rules, or regulations of certain jurisdictions, this may be construed as an advertisement or solicitation.

© 2020 PilieroMazza PLLC
All rights reserved.

About PilieroMazza

PilieroMazza—a business law firm—serves as a strategic partner to government contractors and commercial businesses from across the United States in numerous industries.

We deliver results for our clients by implementing legal and business solutions that take the client’s best interests into consideration. Moreover, PilieroMazza’s efficient operational structure and lean approach to staffing matters translate into competitive pricing for our clients, while providing the highest standard of client service and legal acumen.

PilieroMazza is privileged to represent clients in the following areas:

- Audits & Investigations
- Business & Corporate
- Business Succession Planning
- Corporate and Organizational Governance
- Cybersecurity & Data Privacy
- Debt Financing
- Employee Incentive and Bonus Plans
- False Claims Act
- Government Contracts
- Government Contract Claims & Appeals
- Intellectual Property & Technology Rights
- Labor & Employment
- Labor & Employment for Government Contractors
- Litigation & Dispute Resolution
- Mergers & Acquisitions
- Native American Law & Tribal Advocacy
- Private Equity & Venture Capital

Overview of Legal Considerations

- CMMC in Proposals and Contracts
- Cybersecurity Assessments
- False Claims Act

CMMC in Proposals and Contracts

- Phased rollout approach during the FY2021-FY2-25 period

FY2021	FY2022	FY2023	FY2024	FY2025
15	75	250	325	475

- DoD will specify the required CMMC level in RFIs and RFPs
- CMMC level for subcontractors is dependent upon the type and nature of information flowed down from your prime contractor

NIST SP 800-171 DoD Assessment Methodology

- Means for the DoD to assess contractor implementation of NIST SP 800-171 on contracts that include DFARS clause 252.204-7012
- Transitional self-assessment designed to bridge the gap until the full implementation of CMMC
- Assessment score must be uploaded to the Supplier Risk Management Systems

False Claims Act Considerations

- Violation of the FCA occurs when any person knowingly or recklessly presents a false or fraudulent claim for payment or approval or makes, uses a false record or statement material to a false or fraudulent claim
- Increased relevance in the cybersecurity space and the DoD Assessment and CMMC certification will increase FCA activity
- Potential damages consist of criminal penalties and civil penalties in an amount equal to three times the government's damages as well as \$22,000 per submitted invoice



CYBER CAPITAL
PARTNERS

SOLVING CMMC FOR SMALL BUSINESS



CMMC: Cost Reimbursement

DHG

Bill Walter
Managing Director
Dixon Hughes Goodman
703.970.0509
bill.walter@dhg.com



GOVERNMENT CONTRACTING

WHO IS PAYING FOR ALL THIS?

December 15, 2020

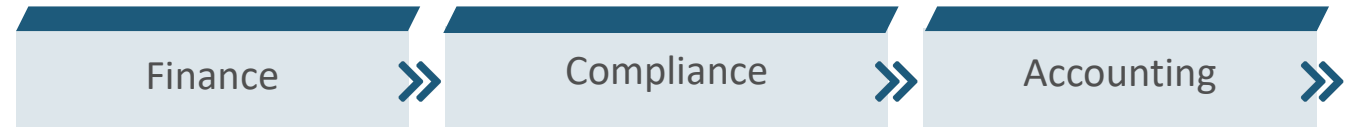
About DHG Government Contracting

DHG's Government Contracting practice provides assurance, tax and consulting services to hundreds of government contractors. Our Government Contracting team is dedicated to working with government contractors across Civilian Federal, Department of Defense and Intelligence Agencies. Key statistics about our practice are outlined below:



This depth of experience and knowledge is beneficial to our government contracting clients in that our group leaders are fully conversant in the requirements applicable to government contractors. We assign experienced Government Contracting professionals to our service teams so they can efficiently navigate this highly technical environment.

In addition to maintaining core accounting service groups for the government contracting industry, **DHG's extensive Government Contract Advisory practice is comprised of former Defense Contract Audit Agency (DCAA) auditors and executives.** Our experienced professionals in this area advise clients in various aspects of finance, accounting and compliance related to government contracting.



Who is paying for all this?

- **Costs of CMMC Readiness and Compliance**
 - General Allowability Requirements – FAR Part 31 – Five Step Test
 - Cost Accounting Practices – Direct, Overhead or G&A?
 - Impact of Contract Type – Cost Reimbursement vs. Fixed Price

- **Government’s Public Cost Estimates in DFARS Rule**
 - Cost per year \$6.7 billion per year
 - Present value over perpetuity - \$92.9 billion to \$224.2 billion
 - Estimates for small and large businesses for each level

What is in the Government's Estimate?

- *Nonrecurring Engineering Costs.* Consists of hardware, software, and the associated labor. The costs are incurred only in the year of the initial assessment.
- *Recurring Engineering Costs.* Consists of any recurring fees and associated labor for technology refresh. The recurring engineering costs associated with technology refresh have been spread uniformly over a 5-year period (i.e. 20% each year as recurring engineering costs).
- *Assessment Costs.* Consists of contractor support for pre-assessment preparations, the actual assessment, and any post-assessment work. These costs also include an estimate of the potential C3PAO costs for conducting CMMC assessment, which are comprised of labor for supporting pre-assessment preparations, actual assessment, and post-assessment work, plus travel cost.
- *Re-certification Costs.* These costs are the same as the initial certification cost.

Small Business Cost Estimate per DoD

CMMC Level	Engineering		Assessment	
	Non-Recurring	Recurring	Contractor Support	C3PAO
1	\$0	\$0	\$1,166	\$1,833
2	\$8,135	\$20,514	\$11,240	\$11,227
3	\$26,214	\$41,666	\$22,479	\$28,616
4	\$938,336	\$301,514	\$33,053	\$37,012
5	\$1,230,214	\$384,666	\$57,292	\$52,799

Based on Journeyman Rate \$83.32/\$99.08 and Senior Rate \$117.08/\$137.72



Our strength lies in our technical knowledge, industry intelligence and future focused approach combined with our drive to help our clients achieve their goals, both today and tomorrow. DHG's professionals are passionate about providing an unparalleled client experience as we listen, innovate and act to help our clients.

TECHNICAL KNOWLEDGE

98%

Clients agree DHG demonstrates significant technical competence

INDUSTRY INTELLIGENCE

10+

Key industries with a depth of industry sector experience and focus, offering industry dedicated assurance, tax and advisory services

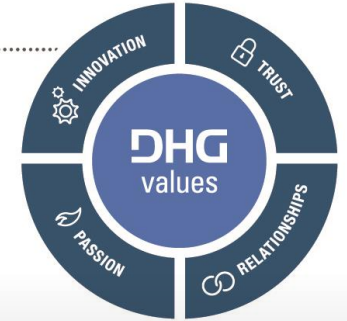
FUTURE FOCUSED

2,000+

People, including more than 300 partners, principals, managing directors and directors committed to innovation

OUR COMMITMENT

DHG's client experience model is driven by the unique needs and goals of each individual client. When we engage with you, we intentionally seek to understand and exceed your expectations by considering your unique, individual goals.



BE RESPONSIVE



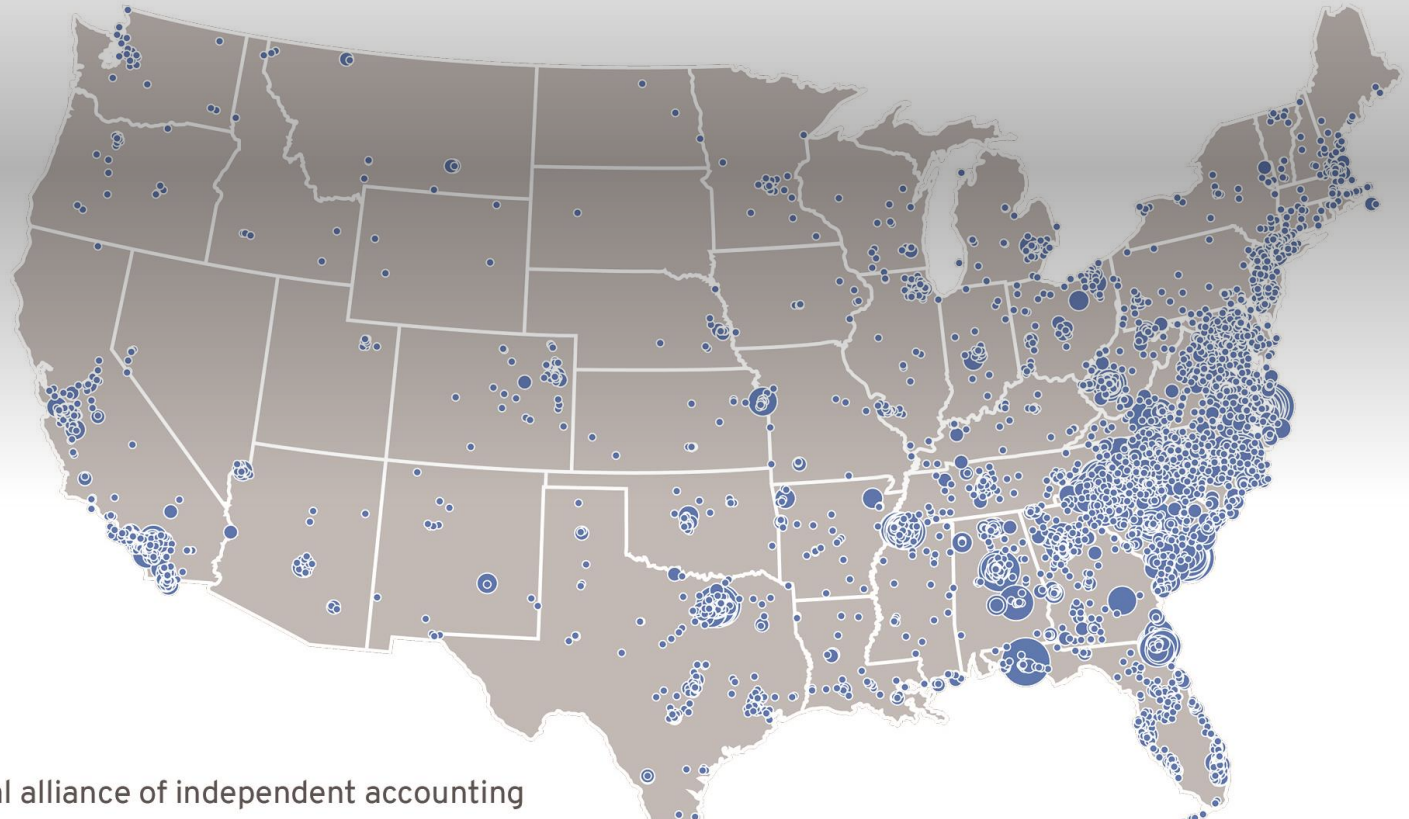
TAKE ACTION



ADD VALUE

NATIONAL FOCUS, GLOBAL ACUMEN

DHG ranks among the top 20 professional services firms in the nation, providing assurance, tax, and advisory services. With more than 2,000 professionals across the United States, the DHG team serves clients in 50 states and internationally.



Member of Praxity™, an international alliance of independent accounting



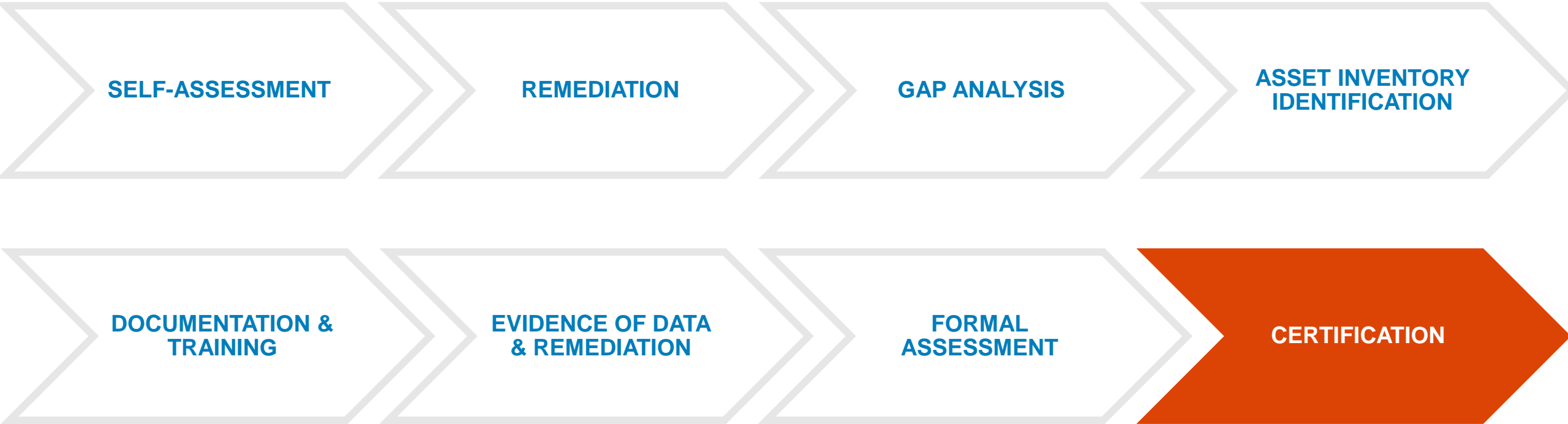
SOLVING CMMC FOR SMALL BUSINESS



Panel Discussion with CMMC Technical Experts



CMMC WORKFLOW



Repeat





Paul Caiazzo, SVP Corporate Development



James Kraemer, CEO



Rick Arthur, CIO & CISO



Ben Gerenstein, President & CEO

Cybersecurity & Consulting Services



250+

CERTIFICATIONS

2500+

CUSTOMERS

20+

YEARS COLLECTIVE

~1M

DEVICES UNDER
MANAGEMENT

14

INDUSTRIES SERVED

2019

YEAR FOUNDED

Portfolio Highlights

PS

Security Assessments

Audit & Compliance
Services

Consulting & Technical
Services

MS

24/7/365 Managed
Detection & Response

Managed SIEM

Managed Zero Trust
Networking

Managed Vulnerability
Scanning

Common CMMC Challenges

- Fully leverage tools & service providers
- Optimize hit to noise ratio
- Who/when/what/where/how data is being used
- Implications for technology strategy
- Compliance pressures
- Hybrid-, multi-cloud, on-premise, etc.
- Visibility into encrypted data directly at the endpoint
- Enabling forensics & response
- Work-from-anywhere
- Resource, expertise and/or bandwidth constraints



Security Maturity

Information Governance

Environment & Endpoint Visibility

Security at Scale

**CMMC Registered Practitioner Organization (RPO)
Assessment & Accreditation App (A3)**

**CMMC Licensed Software Provider (LSP)
CMMC Licensed Partner Publisher (LPP)
CMMC Licensed Training Provider (LTP)**

**CMMC Consulting
CMMC Training
Cybersecurity**

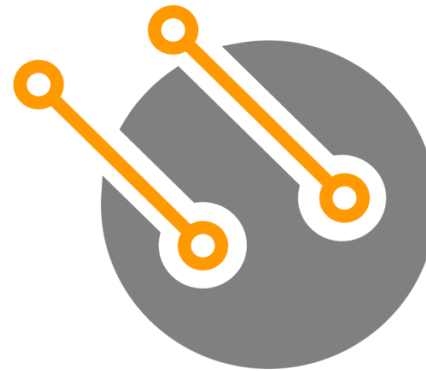
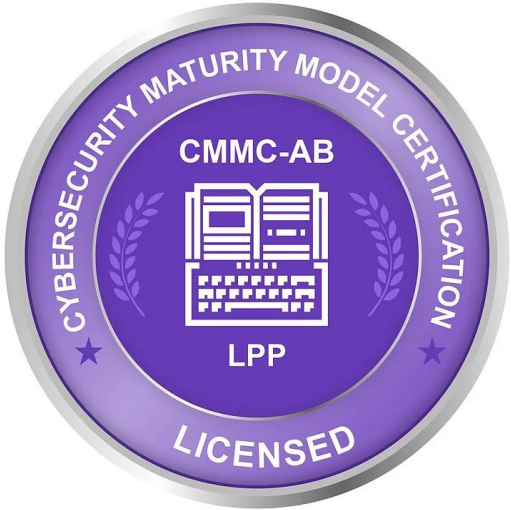


CyberDI
CMMC | Training | Consulting | Solutions

www.cyberdataintelligence.com



@cyberdataintel



CyberDI

< ACCESS CONTROL (AC)

- AC.1.001
- AC.1.002
- AC.1.003
- AC.1.004

AC.1.001

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

Capability

C001 Establish system access requirements

- ARTIFACTS
- AFFIRMATION
- OBSERVATION

Description

Perform Test On

- processes account management on the information system
- automated mechanisms for implementing account management
- automated mechanisms implementing access control policy
- remote access management capability

SAVE

NEXT PRACTICE

Cybersecurity Maturation Model Certification

Do you want to help protect our Global Supply Chain and keep America Safe? Sign up for our Cybersecurity Maturation Model Certification Webinar Serie to Learn How to Do Your Part

[Apply Now](#)



CyberDI



INDEPENDENT

With no vendor bias, Hartman is truly independent and only makes recommendations that are in our clients' best interests.

TRUSTED

Hartman advisors are fellow executives who listen to concerns and keep confidences. We aim to be part of our clients' inner circles.

STRATEGIC

Our clients' goals become our goals, and they drive the creation of roadmaps that focus on both short-and long-term success.

Founded in 2004, Hartman Executive Advisors is an **independent technology advisory firm** that works with business and nonprofit leaders to align IT solutions with business goals and strategy.

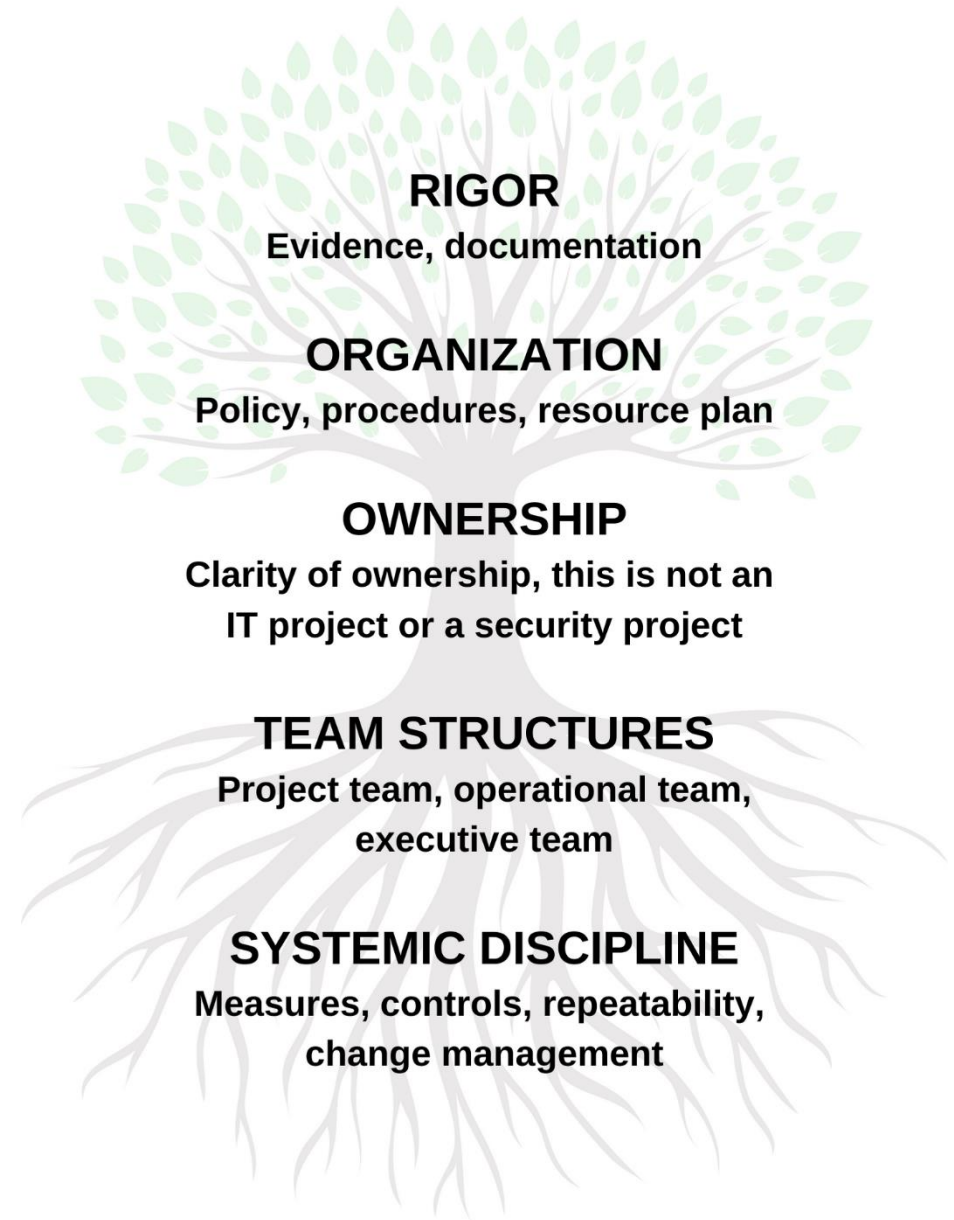
Business and technology are intertwined as never before, and today's leaders are required to make decisions about technology that impact their top and bottom lines.

Hartman's **co-sourced CIO and CISO model** provides the opportunity for executives to work alongside senior IT and cybersecurity advisors who know their industry and their goals. We act as our client's accountable IT leadership, and our clients benefit from leveraging the depth and breadth of a full IT staff at a fraction of the cost while we move the needle on key issues.

How can Hartman help with CMMC readiness?

Hartman's C-level business and technology leaders start by conducting an independent assessment of an organization's readiness for the certification and determine appropriate next steps.

Then, Hartman works directly with leadership to develop a plan to close gaps and work toward certification at the most appropriate level.



**Current DoD Contractor
Cybersecurity Landscape**

- NIST 800-171 Compliance for CUI
- Self-Assessment
- SSP & POAM (Customer generated)
- Compliance in the real world is questionable



**GovCon Enclave
Compliant Data Privacy and Security**

- Robust Holistic Approach with a low cost to implement and maintain
- Collective Defense across your enterprise and your supply chain
- Meets the technical controls of NIST 800-171 and CMMC Level 3

**Future CMMC
Landscape**

- Formal 3rd party assessment required
- No POAM's allowed
- If CUI present 130 practices must be followed
- Cybersecurity maturity must be demonstrated for CMMC Level 3 compliance
- Requirements will soon be mandatory

“Bridges current and future cybersecurity needs”

GovCon Enclave

The Right Solution for CMMC

- Secure, Encrypted Enclave
- Extensive CMMC Compliance Features
- Competent Support
- SOC Services
- Reasonable Cost



C O M P R E H E N S I V E

- Awareness / Training
- Risk / Threat Assessment
- Policies and Procedures
- Access Control
- CMVP-Validated Encryption
- SOC Support
- Enclave Help Desk
- Managed SIEM / MDR
- Enclave IDS / IPS
- Incident Reporting
- Alerting
- Log Management
- Workshops

Compliance Engine

CMMC Simplified

- Extensive Policy Support
- Compliance Dashboard
- Easy Preparation for Formal Assessment
- Compliance Enforcement



- **Compliance Policy Center**
Automates the creation and maintenance of policies, plans and roles to ensure compliance with CMMC and/or NIST 800-171
- **Compliance Management Dashboard**
Delivers situational awareness with clear visual indicators of compliance with applicable CMMC and/or NIST 800-171 controls.
- **Compliance Assessment Prep**
Automates pre-assessment with generation of required documents for formal assessment, including objective evidence.
- **Compliance Enforcer**
Ensures applicable controls are enforced at the boundary and in the enclave with alerts and automated actions in the event of any violations or anomalies.



CYBER CAPITAL
PARTNERS

SOLVING CMMC FOR SMALL BUSINESS



CMMC: Open Q&A



Matthew Condry, CEO



David Shafer, Attorney



Bill Walter, Managing Director



Paul Caiazza, SVP Corporate Development



James Kraemer, CEO



Rick Arthur, CIO & CISO



Ben Gerenstein, President & CEO



SOLVING CMMC FOR SMALL BUSINESS



CMMC Managed Concierge Services, LLC



CMMC CHALLENGES FOR SB GOVCONS



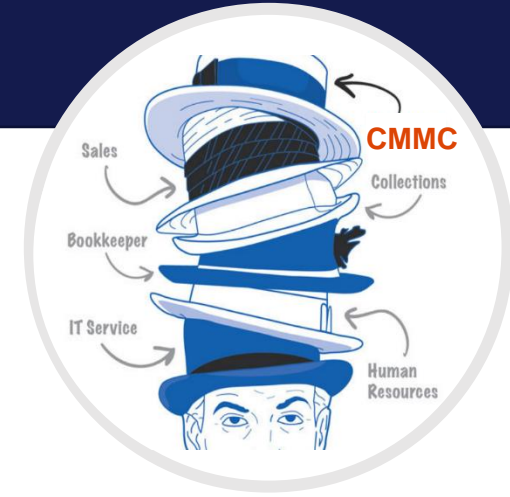
SUPPLY SHORTAGE

- 300,000 contractors
- < 150 CMMC Approved Vendors
- Schedule & Price Uncertainty



CMMC COSTS

- Greater impact on smaller budgets

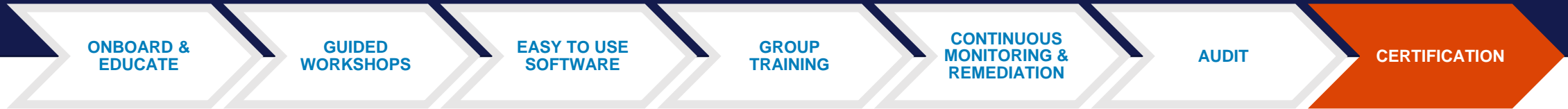


LACK OF INTERNAL RESOURCES

- Compliance team
- Cyber professionals
- Immature processes



MANAGED CONCIERGE SERVICES



PURPOSE BUILT FOR SMALL BUSINESS GOVERNMENT CONTRACTORS

- High Value, Low Cost
- Guide you through CMMC to make sure you avoid costly mistakes
- Manage Suppliers & Vendors



GUIDED WORKSHOP SERIES



**Many will want
to perform
tasks in house
to save \$\$.**

*Why go
alone?*

MONTHLY 2-HOUR WORKSHOPS

- Guided walk through of each of the topics
- Access to CMMC experts
- All Questions Answered
- Knowledge Center (text & video)

\$499 Annual Subscription

With 20% discount code for today's participants, \$399





CYBER CAPITAL
PARTNERS

SOLVING CMMC FOR SMALL BUSINESS



Closing Remarks



Additional Information

Links to the video of today's event will be on www.cybercp.com

Jason Gayl

Managing Partner

Jason@cybercp.com

202-329-2377

Doug Black

Partner

Doug@cybercp.com

703-402-4511

