



SecureTheVillageTM

Preparing for CMMC Certification ... Covid-19 Update

April 9, 2020

It Takes the Village to Secure the VillageTM


**This SecureTheVillage Webinar brought to
you by our Platinum Sponsor / Investor**

2



Preparing for CMMC Certification

- Guide: Stan Stahl, PhD
 - ▣ Founder, SecureTheVillage
 - ▣ President, Citadel Information Group

- Guest:  **ARIENTO**
 - ▣ Chris Rose MBA CSCS CISSP CISM
 - ▣ Managing Partner, Ariento
 - ▣ Board of Directors, SecureTheVillage

Outline



- Status update on the CMMC roll out: what to expect and how/when it will apply to your organization
- How has/will COVID-19 affect CMMC roll out?
- What is CMMC and how is it different from DFARS 7012 and NIST 800-171 ?
- What should you be doing now to prepare for CMMC ?
- What does CMMC mean for the future of cyber compliance ?

You will see CMMC by end of fiscal year

5

- CMMC-AB formed in February
 - ▣ Signed MOU with DoD at end of March
- CMMC Model v1 released Jan 31
 - ▣ v1.02 release March 20
- C3PAO certifications begin in Q2 of 2020
 - ▣ Pilot group end of April
- CMMC in 10 contracts, ~1,000 contractors by Sep 30
 - ▣ CMMC in RFIs in Summer 2020
 - ▣ CMMC in RFPs in Fall 2020

COVID-19 impact on CMMC has been minimal

6

- Training of pilot auditors experienced some delays due to inability to meet in person
- “We, all of us that are mission-essential, have been working on COVID-19, but, although we are working diligently to ensure we are doing our best in the Department of Defense to save lives, work does continue and we are not slowing our roll at all.”
 - - Katie Arrington
- “CMMC remains a priority for the department, and Ms. Katie Arrington continues to work closely with the accreditation body and industry. We don’t anticipate any impacts to the CMMC timeline due to COVID-19, but with the social distancing guidelines we are postponing any public events.”
 - - Department spokesman Lt Col Mike Andrews

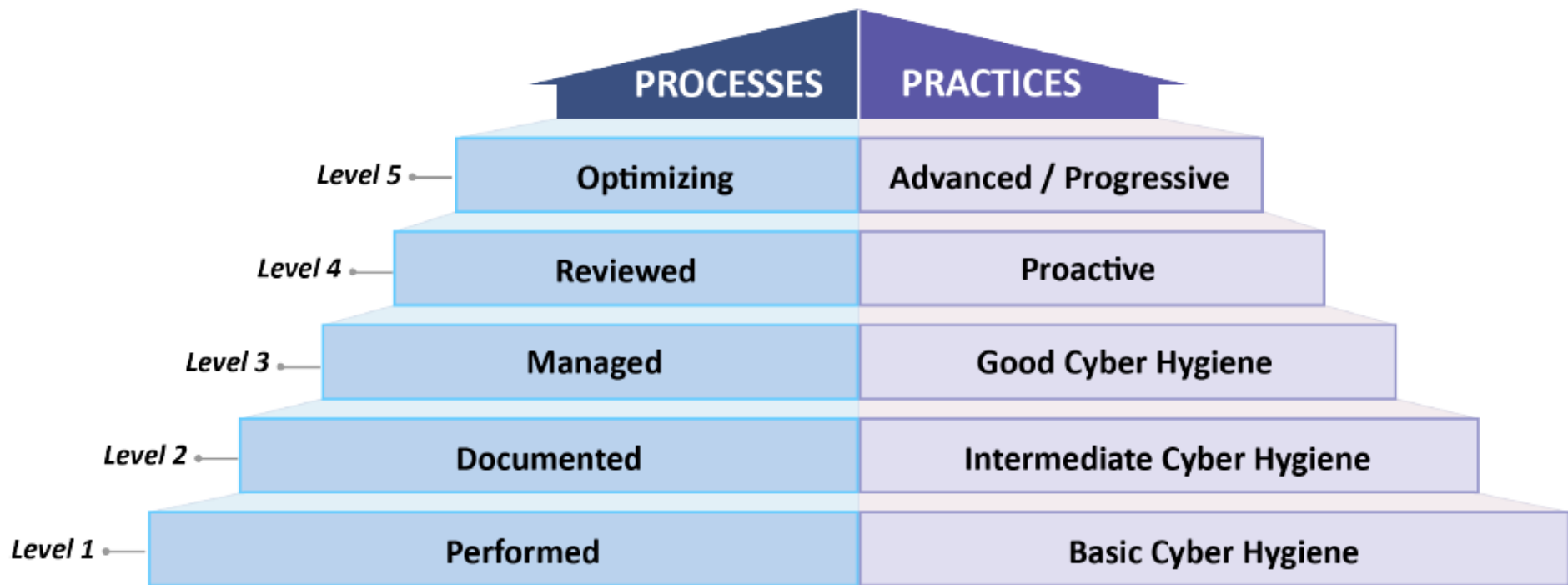
CMMC vs. NIST 800-171

7

- ❑ Self-Attestation vs. Independent Audit
- ❑ One size fits all vs. 5 levels
- ❑ 110 security controls vs. 171 processes and practices
 - ▣ 130 controls in CMMC Level 3, maps directly to NIST
- ❑ 14 vs. 17 domains
 - ▣ 43 capabilities in CMMC
- ❑ SSP/POAM vs Certify where you are at
- ❑ FCI and CUI
- ❑ Allowable costs

Demonstrate institutionalization of processes & implementation of practices

8



Estimated resources to achieve compliance

9

Level Of Effort:

Low (L) – Under 40 hours to implement; (1) PTE to maintain

Medium (M) – 40-100 hours to implement, (1) FTE to maintain

High (H) – 100+ hours to implement, Multiple FTE to maintain

Cost (Materials):

Cheap (\$) – Under \$500/user/year

Balanced (\$\$) – \$501-\$2,000/user/year

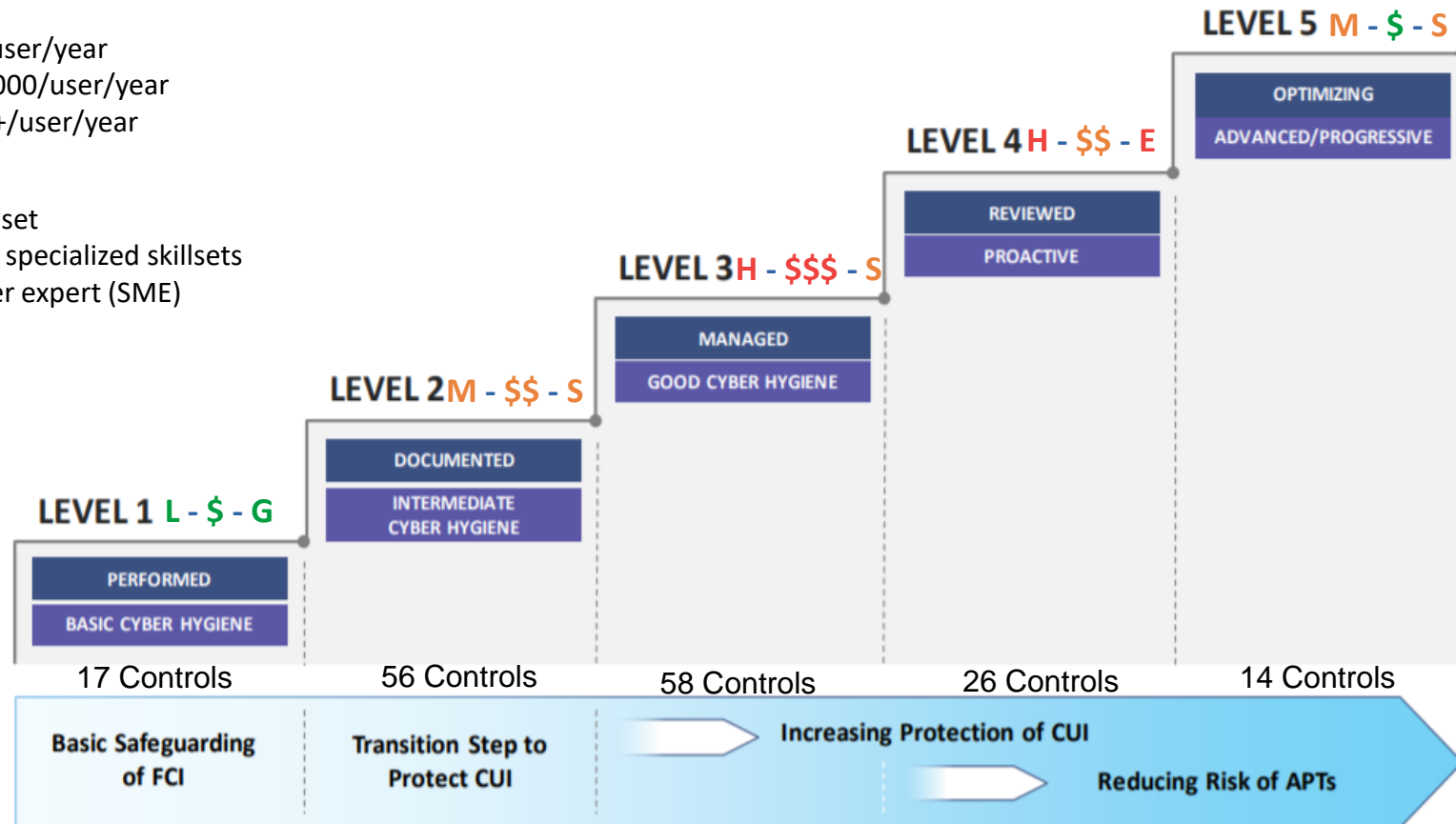
Expensive (\$\$\$) – \$2,000+/user/year

Skillset Required:

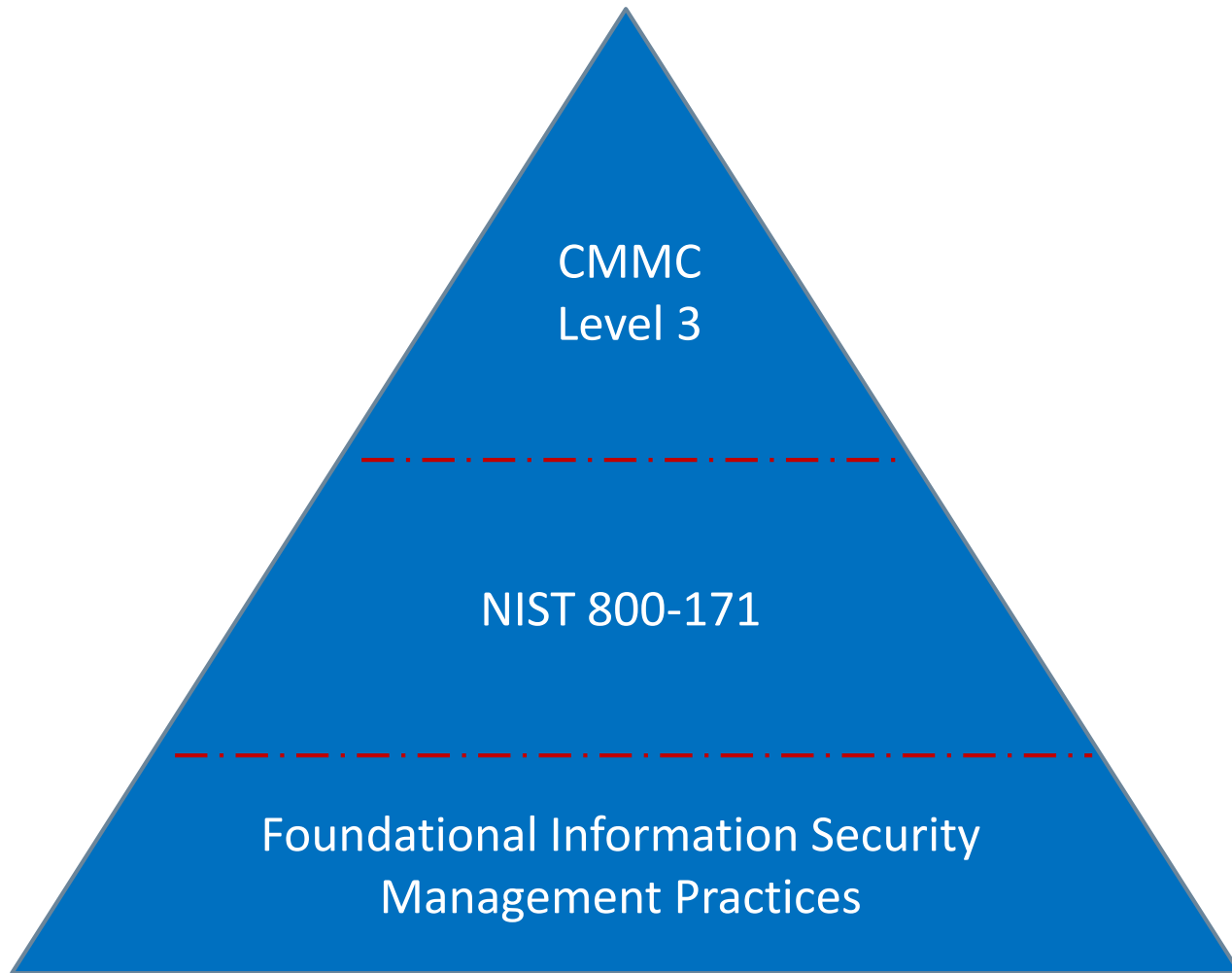
General (B) – General skillset

Specialized (S) – Multiple, specialized skillsets

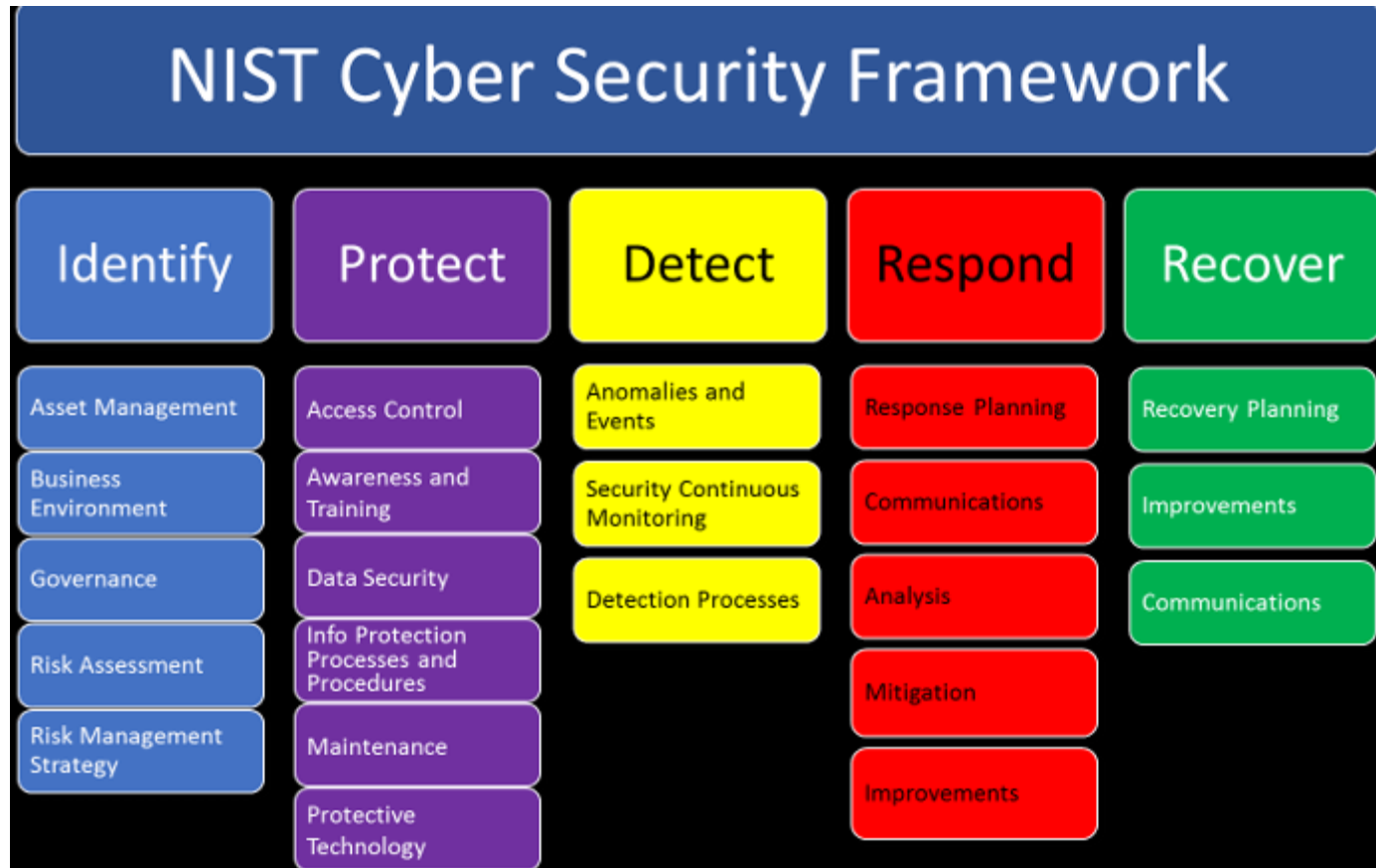
Expert (E) – Subject matter expert (SME)



Getting Ready for CMMC: Building the Foundation



NIST Cyber Security Framework is Foundational



Center for Internet Security 20 Foundational Controls

12



V7

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

Foundational Information Security Management Practices

13

Information Security
Management

Security
Management of IT
Interface

Information
Resilience

Subject Matter
Expertise

Security
Management of the
IT Infrastructure

Information Security
Governance

Security Management
of Sensitive/Private
Information

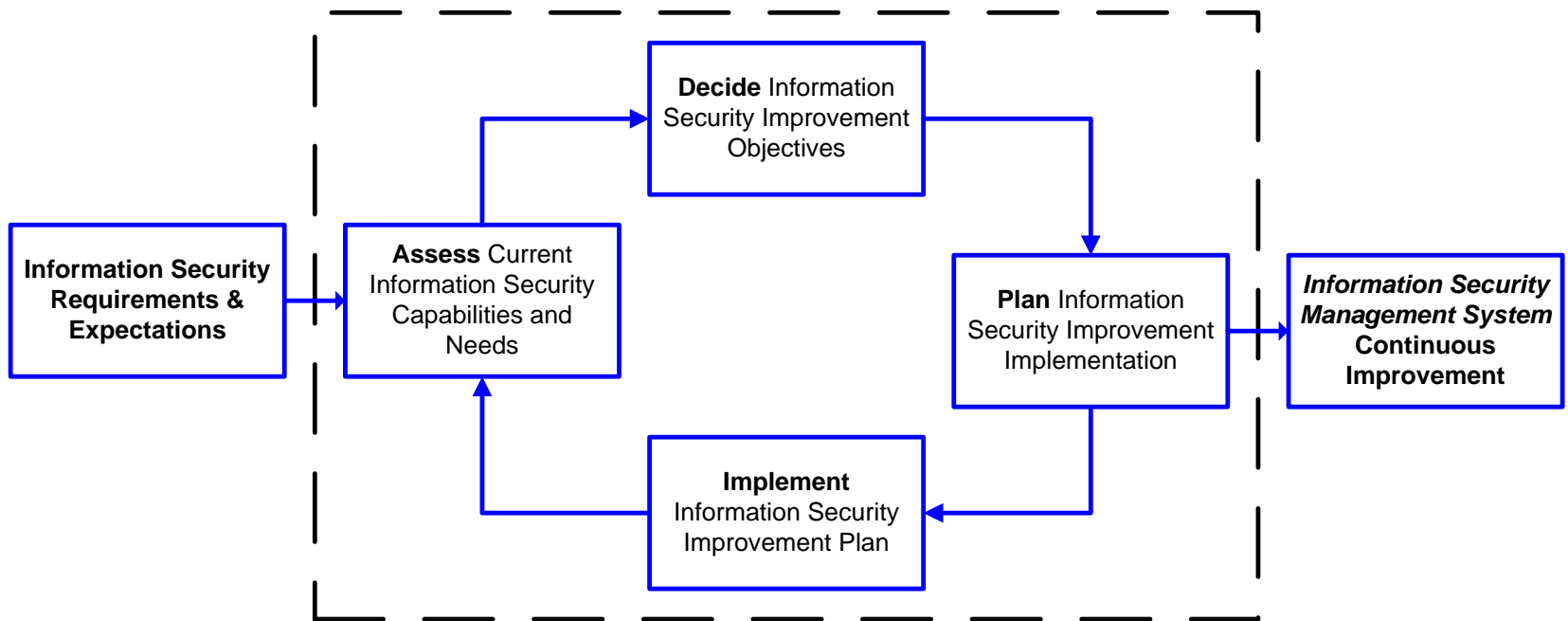
3rd-Party Security
Assurance

Secure the Human

*SecureTheVillage Minimum Reasonable Information
Security Practices: <https://mrsp.securethevillage.org/>*

As Threats Increase, So Must Defenses: A Spiral Model of Continuous Improvement

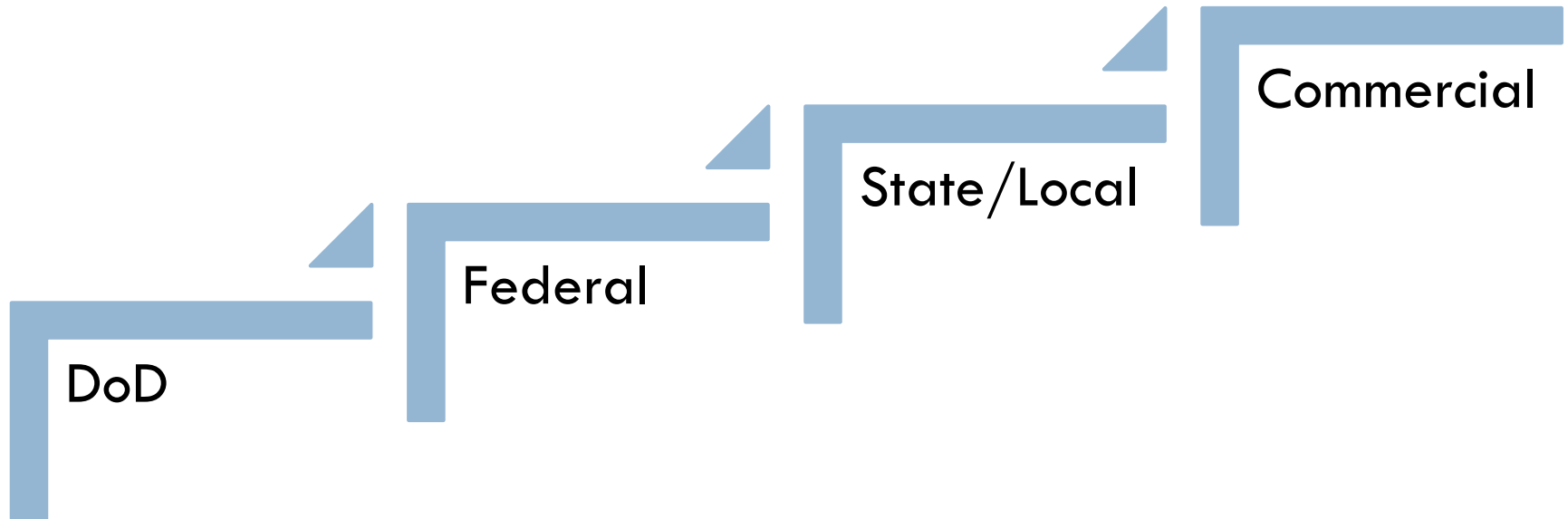
14



Spiral Model is a Service Mark of Miller Kaplan.

Can CMMC become the single standard?

15



CMMC Resources

16

- <https://CMMCmarketplace.com>
 - ▣ Follow on social media
 - ▣ Sign up for newsletter
- <https://CMMCab.org>
 - ▣ Sign up for newsletter
- <https://www.acq.osd.mil/cmmc>
- <https://www.UpOnCyber.com>
 - ▣ Register to be notified when conference registration is available



Appendices: Domains and Capabilities

17 Domains

18



43 capabilities

19

Domain	Capability
Access Control (AC)	<ul style="list-style-type: none">• Establish system access requirements• Control internal system access• Control remote system access• Limit data access to authorized users and processes
Asset Management (AM)	<ul style="list-style-type: none">• Identify and document assets
Audit and Accountability (AU)	<ul style="list-style-type: none">• Define audit requirements• Perform auditing• Identify and protect audit information• Review and manage audit logs
Awareness and Training (AT)	<ul style="list-style-type: none">• Conduct security awareness activities• Conduct training
Configuration Management (CM)	<ul style="list-style-type: none">• Establish configuration baselines• Perform configuration and change management
Identification and Authentication (IA)	<ul style="list-style-type: none">• Grant access to authenticated entities
Incident Response (IR)	<ul style="list-style-type: none">• 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)	<ul style="list-style-type: none">• Manage maintenance

43 capabilities continued

20

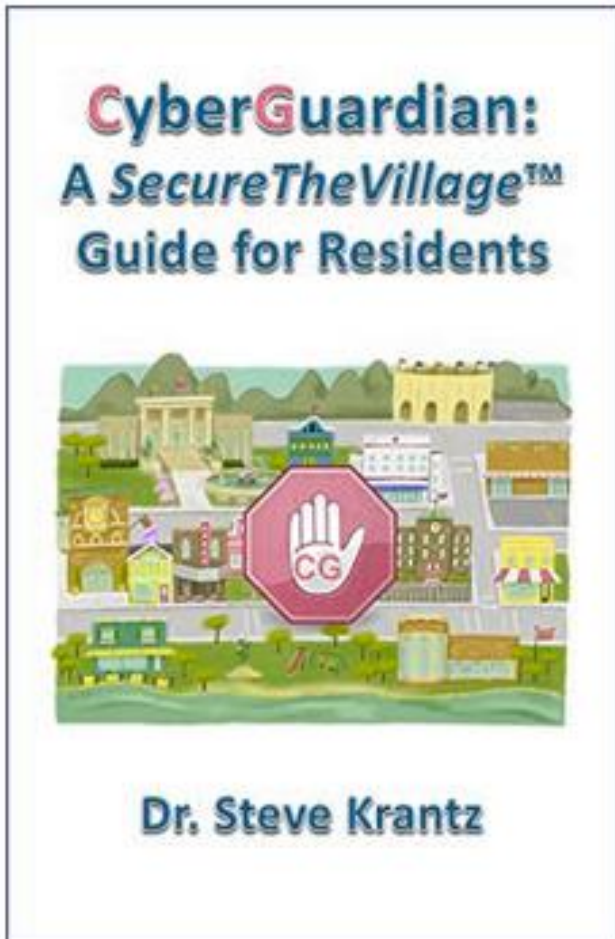
Media Protection (MP)	<ul style="list-style-type: none">• Identify and mark media• Protect and control media• Sanitize media• Protect media during transport
Personnel Security (PS)	<ul style="list-style-type: none">• Screen personnel• Protect CUI during personnel actions
Physical Protection (PE)	<ul style="list-style-type: none">• Limit physical access
Recovery (RE)	<ul style="list-style-type: none">• Manage back-ups
Risk Management (RM)	<ul style="list-style-type: none">• Identify and evaluate risk• Manage risk
Security Assessment (CA)	<ul style="list-style-type: none">• Develop and manage a system security plan• Define and manage controls• Perform code reviews
Situational Awareness (SA)	<ul style="list-style-type: none">• Implement threat monitoring
Systems and Communications Protection (SC)	<ul style="list-style-type: none">• Define security requirements for systems and communications• Control communications at system boundaries
System and Information Integrity (SI)	<ul style="list-style-type: none">• Identify and manage information system flaws• Identify malicious content• Perform network and system monitoring• Implement advanced email protections

SecureTheVillage Webinar Series

21

- Information Security Management Guidance
 - ▣ Practical
 - ▣ Real-World
 - ▣ How-To
 - ▣ Actionable
- SecureTheVillage ResourceKit
- Second Thursday of month, 10AM Pacific

Next Webinar: May 14: Securing Your Home & Family, Part 1



**Dr. Steve Krantz, Author
*CyberGuardian: A SecureTheVillage™
Guide for Residents***

Interested in Cybersecurity? Please Get Involved!!! Join Our Village!!!

23

Follow SecureTheVillage on LinkedIn

<https://www.linkedin.com/company/secure-the-village>

Get Our Free *Cybersecurity News of the Week, with Weekend Vulnerability & Patch Report*

<https://securethevillage.org/>

Attend a (Virtual) Event: Conversations in Cybersecurity Webinars, Town Halls, Happy Hours

<https://securethevillage.org/events/>

Join the SecureTheVillage Leadership Council

<https://securethevillage.org/about/leadership-council/>

<https://securethevillage.org/about/leadership-council-faq/>

Co-Host a (Virtual) Event

Email us at info@securethevillage.org. Put *Co-Host Event* in Subject

For More Information ...

24

Stan Stahl, SecureTheVillage & Miller Kaplan

Stan@SecureTheVillage.org

@stanstahl

323-428-0441

Chris Rose, MBA CSCS CISSP CISM, Managing Partner, Ariento

chris@ariento.com

323-510-5124

FREE *Cybersecurity News of the Week & Weekend Vulnerability and Patch Report*

<https://SecureTheVillage.org>



Preparing for CMMC Certification

Thank You!

It Takes the Village to Secure the Village™