ATI
ADVANCED TECHNOLOGY INTERNATIONAL ®

CMMC 1.0 Level 3 Review

February 20, 2020

SUMMIT7

SUMMIT7

Cybersecurity Maturity Model Certification 1.0 Level 3 Review

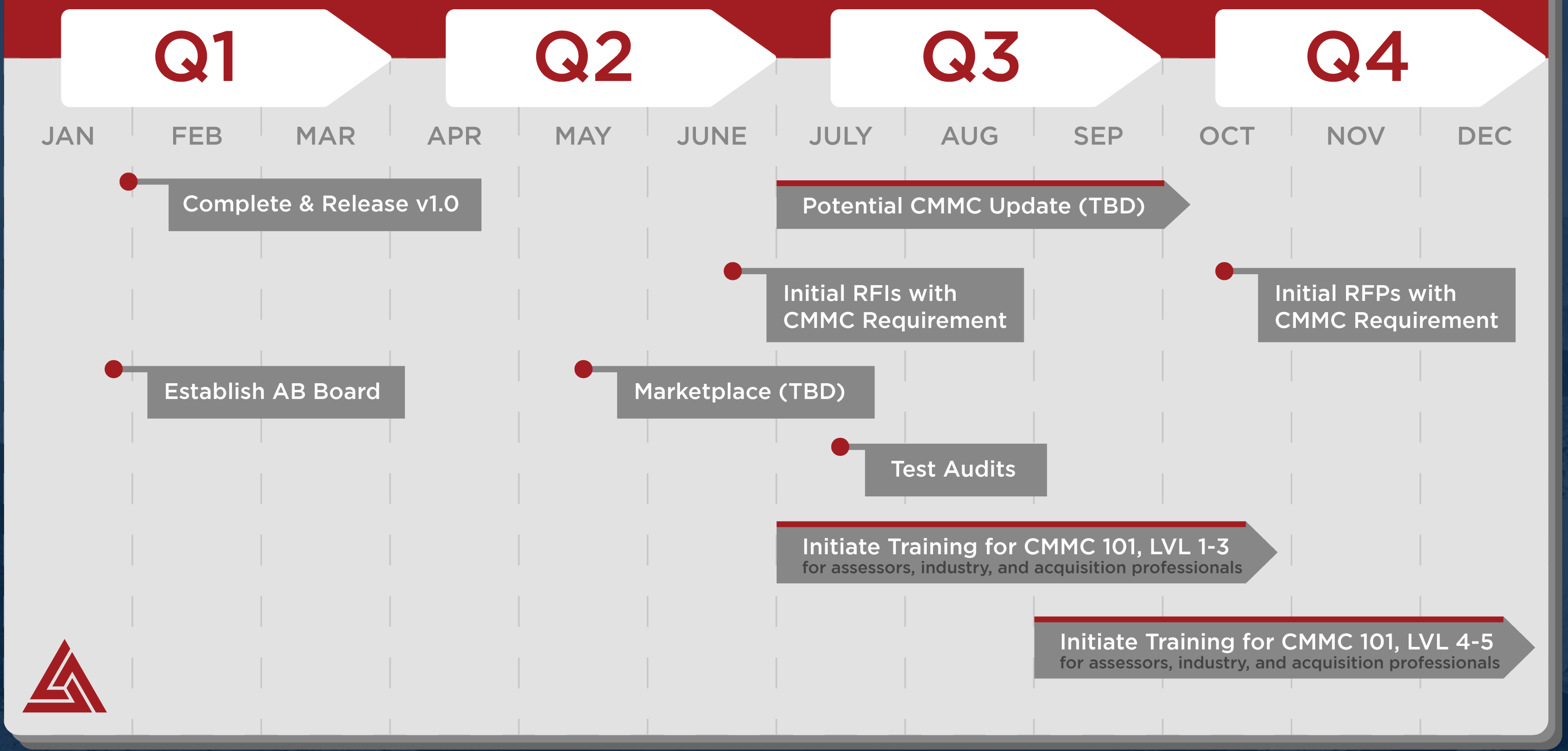
February 20, 2020

Agenda

- Introductions
- CMMC Schedule
- CMMC 1.0 and Level 3 Overview
- The Big 20!
- Potential Technical Solutions
- Cost and Project Considerations
- Q&A

SUMMIT7

2020 CMMC SCHEDULE



Q1 Q2 Q3 Q4

JAN FEB MAR APR MAY JUNE JULY AUG SEP OCT NOV DEC

Complete & Release v1.0

Potential CMMC Update (TBD)

Initial RFIs with CMMC Requirement

Initial RFPs with CMMC Requirement

Establish AB Board

Marketplace (TBD)

Test Audits

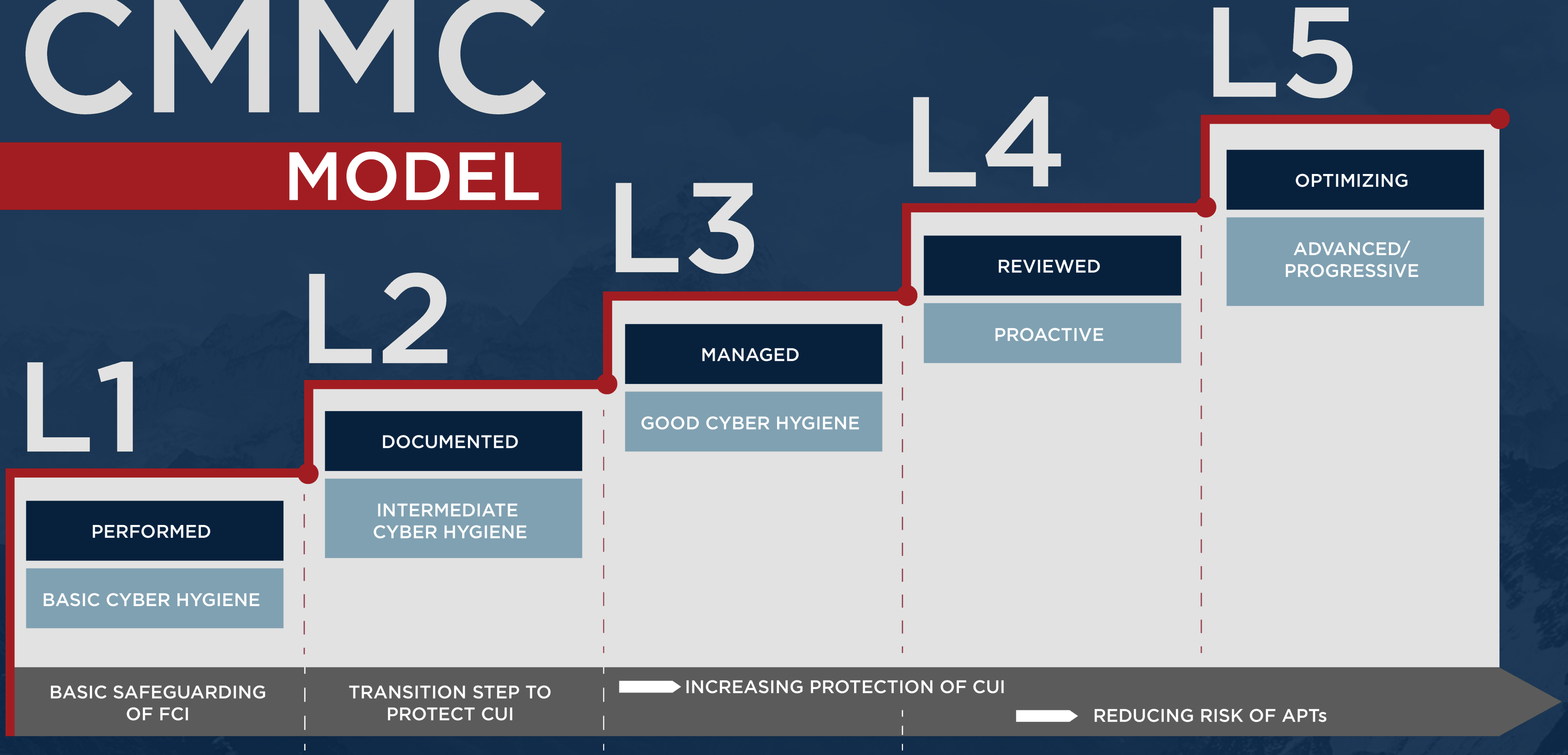
Initiate Training for CMMC 101, LVL 1-3
for assessors, industry, and acquisition professionals

Initiate Training for CMMC 101, LVL 4-5
for assessors, industry, and acquisition professionals

SUMMIT7

CMMC Overview

CMMC MODEL



L1

PERFORMED

BASIC CYBER HYGIENE

L2

DOCUMENTED

INTERMEDIATE CYBER HYGIENE

L3

MANAGED

GOOD CYBER HYGIENE

L4

REVIEWED

PROACTIVE

L5

OPTIMIZING

ADVANCED/ PROGRESSIVE

BASIC SAFEGUARDING OF FCI

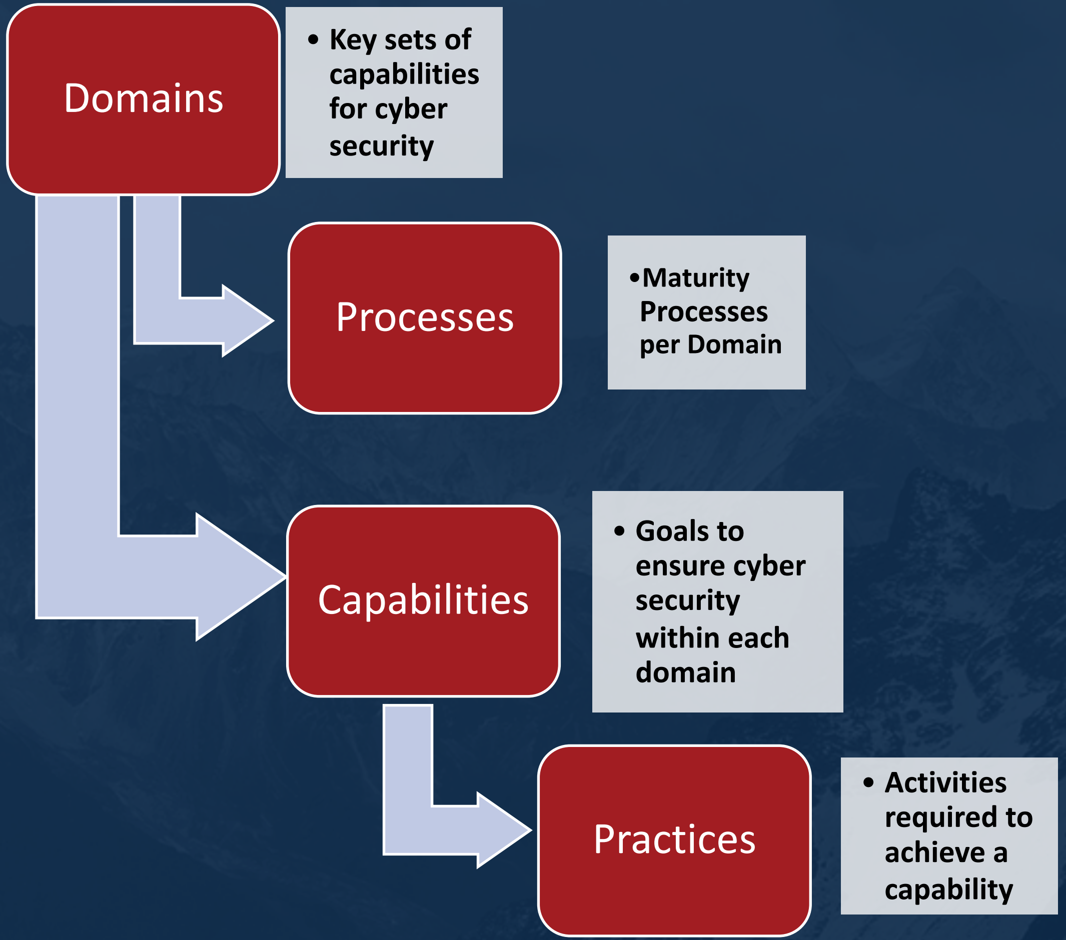
TRANSITION STEP TO PROTECT CUI

INCREASING PROTECTION OF CUI

REDUCING RISK OF APTs

CMMC Model Framework

- 17 Domains consisting of Capabilities
- Capabilities include multiple Practices and Processes, each assigned to a specific Level 1-5
- Capabilities Numbered C001 – C043
- Practice Numbering Methodology
  - XX.#.***
  - XX = 2 Letter Domain (AC = Access Control)
  - # = CMMC Level
  - *** = Practice Number
  - AC.1.001 = "Limit Information system access…"



Domains

- Key sets of capabilities for cyber security

Processes

- Maturity Processes per Domain

Capabilities

- Goals to ensure cyber security within each domain

Practices

- Activities required to achieve a capability

CMMC Practices

Level 1	• 17 Practices
Level 2	• 55 Practices
Level 3	• 58 Practices
Level 4	• 26 Practices
Level 5	• 15 Practices

- Level 1 – 3 Includes 130 Practices and are targeted at the largest and most active component of the DIB
- Level 4-5 Includes 41 additional Practices and are targeted toward a small subset of the DIB supporting critical programs

CMMC Processes

Level 1	• 0 Processes
Level 2	• 34 Processes
Level 3	• 17 Processes
Level 4	• 17 Processes
Level 5	• 17 Processes

Follow the pattern of

Level 2

- Establish a policy that includes [DOMAIN]
- Document the CMMC practices to implement [DOMAIN] Policy

Level 3

- Establish, maintain and resource a plan that includes [DOMAIN]

Level 4

- Review and measure [DOMAIN] activities for effectiveness

Level 5

- Standardize and optimize a documented approach for [DOMAIN] across all applicable organizational units

SUMMIT7

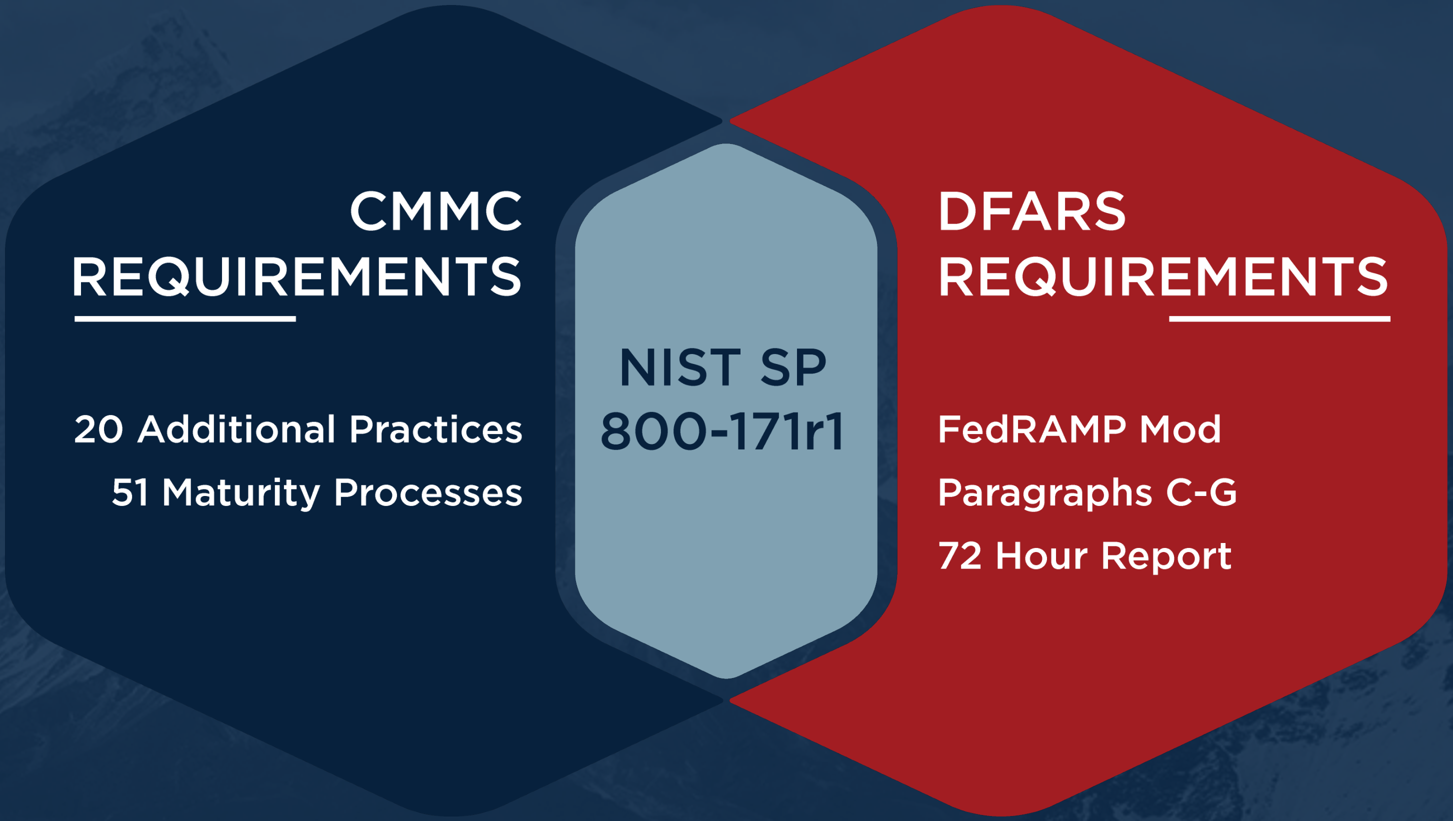
CMMC Source Material

- NIST 800-171r1
- FAR Clause 52.204
- DRAFT SP 800-171B
- CIS Controls v7.1
- NIST Cybersecurity Framework 1.1
- CERT Resilience Management Model 1.2
- NIST SP 800-53 Rev 4
- AU ACSC Essential Eight
- UK NCSC Cyber Essentials
- CMMC Working Group
- **Dropped ISO 27001**

SUMMIT7

How Do DFARS and CMMC L3 Overlap?

- RFI / RFP Stage
  - CMMC Level Identified in the RFI/RFP
- Contract Award
  - Must have a successful C3PAO CMMC Audit
  - DFARS Requirements Identified in Contract
  - Must Agree to Abide by DFARS 252.204-7012 Requirements in the Representations and Certifications
- Don’t forget about DFARS 252.204-7012
  - DCMA Audits are coming!



CMMC REQUIREMENTS

20 Additional Practices

51 Maturity Processes

NIST SP 800-171r1

DFARS REQUIREMENTS

FedRAMP Mod

Paragraphs C-G

72 Hour Report

SUMMIT7

What kind of failures do we see?

- NIST Technical Controls
  - Lack of Multifactor Authentication to the Desktop
  - No Server or Desktop Baseline Configurations
  - No Centralized Audit Logging and Retention
  - Users with Administrative Access
  - No Application Blacklisting / Whitelisting
  - Separation of Duties and Least Privilege

- DFARS Requirements
  - No Medium Assurance Certificate / Token
  - Leveraging Non FedRAMP Cloud Solutions
  - Leveraging Cloud Solutions that don’t meet 252.204-7012 Paragraphs C-G

- NIST Procedural Controls and Documentation
  - No Change Management or Change Logs
  - CUI Data Flow Diagrams
  - Risk Management / Mitigation Plans
  - Incident Response Plan and Testing

SUMMIT7

What will it take to get CMMC Certified?

- Level 1:
  - 17 NIST 800-171 Requirements
- Level 2:
  - 72 Practices (65 NIST 800-171 Requirements PLUS 7 Other Practices)
  - 34 Maturity Processes
- Level 3:
  - 130 Practices (110 NIST 800-171 Requirements PLUS **20 Other Practices**)
  - 51 Maturity Processes
- Level 4:
  - 156 Practices (110 NIST 800-171 Requirements PLUS 46 Additional Practices)
  - 68 Maturity Processes
- Level 5:
  - 171 Practices (110 NIST 800-171 Requirements PLUS 61 Additional Practices)
  - 85 Maturity Processes
- System Security Plans and POA&Ms are still required
  - POA&Ms will not be honored for 3rd Party Audits
  - Must fully meet all Level 3 requirements at the time of the Audit

- DFARS and CMMC L3 Certification Process
  - Leverage only FedRAMP Moderate + Cloud Solutions
  - Ensure you can meet Paragraphs C-G
  - Build to NIST 800-171 Standards
  - Implement 20 Additional CMMC Practices
  - Build NIST and the 51 Maturity Processes
  - Ensure SSP is up to date
  - Schedule with C3PAO for Audit
- New Technical Solutions / Requirements
  - Security Information & Event Management (SIEM) Solution
  - Backup / Restore Solution
  - DNS Filtering
  - Isolate Unsupported Platforms
  - Secure Management Protocols
  - SPAM / Email Protections

SUMMIT7

CMMC Notes

- Certification will not be required for existing Contracts
- Company must have a "CMMC 3rd Party Assessment Organization" (C3PAO) certification prior to contract award.
- Certifications will be good for 3 Years
- Expectation of 10 Contracts with 150 total companies per contract in 2020. Total of 1,500 Companies
- Focus contracts will include Nuclear, Missile Defense, OTAs, SBIRs and STRs.
  - SOCOM is providing $6,500 in Technical and Business Assistance (TABA) funding toward CMMC Level 1 as part of their Phase 1 SBIR
- Small Businesses should look to the PTACs for potential assistance
- Phased rollout of CMMC into Contracts through 2025. All new contracts in 2026 will have CMMC requirements.
- The CMMC Working Group / Accreditation Board may begin making modifications to the CMMC Practices and Processes as soon as Fall 2020.
- DFARS 252.204-7012 Changes are coming later in 2020.
- DODI 5000 series changes are coming in 2020

SUMMIT7

SUMMIT7

The Big 20!

Microsoft

The Big 20!

10 Technical and 10 Procedural Practices to Implement to get to Level 3

1. AM.3.036: Define procedures for the handling of CUI data
2. AU.2.044: Review Audit Logs
3. AU.3.048: Collect audit information (e.g., logs) into one or more central repositories
4. IR.2.093: Detect and Report Events
5. IR.2.094: Analyze and triage events to support event resolutions and incident declaration
6. IR.2.096: Develop and Implement responses to declared incidents according to predefined procedures
7. IR.2.097: Perform root cause analysis on incidents to determine underlying causes
8. RE.2.137: Regularly perform and test data backups
9. RE.3.139: Regularly perform complete and comprehensive and resilient data backups as organizationally defined
10. RM.3.144: Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources and risk measurement criteria.

SUMMIT7

The Big 20!

10 Technical and 10 Procedural Practices to Implement to get to Level 3

11. RM.3.146: Develop and implement risk mitigation plans
12. RM.3.147: Manage non-vendor supported products (e.g. end of life) separately and restrict as necessary to reduce risk.
13. CA.3.162: Employ a security assessment of enterprise software that has been developed internally, for internal use, and that has been organizationally defined as an area of risk. (MODIFIED)
14. SA.3.169: Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.
15. SC.2.179: Use encrypted sessions for the management of network devices
16. SC.3.192: Implement DNS filtering services
17. SC.3.193: Implement a policy restricting the publication of CUI on publicly accessible websites (e.g. Forums, LinkedIn, Facebook, etc.)
18. SI.3.218: Employ spam protection mechanisms at information system access entry and exit
19. SI.3.219: Implement email forgery protections (ADDED)
20. SI.3.220: Utilize email sandboxing to detect or block potentially malicious email attachments

SUMMIT7

Asset Management /Audit and Accountability

AM.3.036: Define procedures for the handling of CUI data

- Procedural Requirement
- Accounts for Digital and Physical CUI
- Include guidance on receiving, transmitting, storing and destroying CUI

AU.2.044: Review Audit Logs

- Procedural Requirement / Technical Enhancement
- Level of Review may be determined by a Risk Assessment

AU.3.048: Collect audit information (e.g., logs) into one or more central repositories

- Technical Requirement
- Implement a Security Information and Event Management Solution.
- Preferably a single Repository

SUMMIT7

Incident Response

IR.2.093: Detect and Report Events

- Procedural Requirement / Technical Enhancement
- Individuals Can Detect Breakdowns and Report Events
- Monitor Automated Alerts / Alarms
- Leverage the SIEM capability

IR.2.094: Analyze and triage events to support event resolutions and incident declaration

- Technical Requirement
- Evaluate if events are related
- Determine if an event should be escalated
- Determine if you should declare an incident
- Leverage the SIEM capability

IR.2.096: Develop and Implement responses to declared incidents according to predefined procedures

- Procedural Requirement
- Write an Incident Response Procedure
  - Contain Damage
  - Communicate to Users / Stakeholders
  - Implement Controls

IR.2.097: Perform root cause analysis on incidents to determine underlying causes

- Procedural Requirement
- Develop a Root Cause Analysis on each Incident
- Determine the Administrative, Technical and Physical Control Weaknesses
- Capture Lessons Learned
- Initiate Improvements to avoid future incidents

SUMMIT7

Recovery

RE.2.137: Regularly perform and test data backups

- Technical Requirement
- Determine Backup Requirements
- Develop Backup Solution for All System and Data Storage Locations
- Execute Backups to Controlled Locations
- Test Backups on a Regular Basis

RE.3.139: Regularly perform complete and comprehensive and resilient data backups as organizationally defined

- Technical Requirement
- Define Organizational Requirements
- Develop Resilient Infrastructure to protect against physical disaster or malicious attack
- Comprehensive backups cover all systems necessary for business effectiveness or continuity
  - Servers / Line of Business Systems
  - Key Workstations / Control Systems
  - Cloud / Collaboration Systems (Office 365)

SUMMIT7

Risk Management

RM.3.144: Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources and risk measurement criteria.

- Procedural / Documentation Requirement
- Extension of RM.2.141
- Define a Risk Assessment Schedule
- Ensure the following are included
  - Risk Categories (Threats)
  - Sources of Risk
  - Risk Measurement Criteria
- Includes Quantitative and Qualitative Data

RM.3.146: Develop and implement risk mitigation plans

- Procedural / Documentation Requirement
- Define a Mitigation Plan for each Risk
  - Reduce the threat
  - Limit exposure / Identify controls
  - Staff and Resource the plan
  - How to Execute the Plan
  - Measure the Results
- Possible Risk Dispositions include
  - Avoid / Accept
  - Monitor / Defer
  - Transfer / Mitigate

RM.3.147: Manage non-vendor supported products (e.g. end of life) separately and restrict as necessary to reduce risk.

- Technical Requirement
- Determine Risk Exposure
- Leverage Extended Support if possible
- Isolate unsupported products within your environment
- Upgrade / Replace / Retirement

SUMMIT7

Security Assessment / Situational Awareness

CA.3.162: Employ a security assessment of enterprise software that has been developed internally, for internal use, and that has been organizationally defined as an area of risk.

- Procedural / Technical Requirement
- New Practice / Replaced Code Reviews
- May do Manual Code Reviews against Secure Development Guidelines
  - Use a separate development team
- May Leverage Static or Dynamic Testing Tools
- Do not allow the code on the network until the review and mitigations are complete

SA.3.169: Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.

- Procedural / Technical Requirement
- Ensure the Organization is receiving Threat Information from high quality sources
- Subscribe to information feeds from organizations like
  - US-CERT
  - ISACA
  - ICS-CERT
  - Industry Associations / Vendors
  - DoD
  - Infragard
- Ensure information is reviewed and briefed to stakeholders within the organization

System and Communication Protection

SC.2.179: Use encrypted sessions for the management of network devices

- Technical Requirement
- Only use encrypted sessions when Managing Network Devices
- Secure Shell (SSH), HTTPS or TLS are preferred.
- Encrypted VPNs may also be an option.
- Do not use unencrypted protocols such as Telnet, HTTP, SNMPv1 or 2, Cisco SMI

SC.3.192: Implement DNS filtering services

- Technical Requirement
- Prevents access to known malicious websites
- Prevents users from receiving IPs for blocked domains.
- Options May include:
  - DNS Policies on Windows Server / Linux Server
  - OpenDNS
  - Cloud services (Check for Compliance)
  - Hardware based Devices

SC.3.193: Implement a policy restricting the publication of CUI on publicly accessible websites (e.g. Forums, LinkedIn, Facebook, etc.)

- Procedural Requirement
- Establish a policy that restricts individuals from posting CUI on websites and social media
- Review Policy regularly
- Include this information in your annual security training

SUMMIT7

System and Information Integrity

SI.3.218: Employ spam protection mechanisms at information system access entry and exit

- Technical Requirement
- Implement on both inbound and outbound email
- Helps protect against SPAM, Phishing, Viruses and Malware
- Options May include
  - Hardware based Devices
  - Cloud Services (check for compliance)
  - Server based SPAM Filters
- Individual User Managed Quarantines would be an usability enhancement

SI.3.219: Implement email forgery protections (ADDED)

- Technical Requirement
- Protects the environment against Phishing and other email based threats
- Always implement email protections on your deliverable domains. These solutions may include:
  - Sender Policy Framework (SPF Records)
  - Domain Keys Identified Mail (DKIM)
  - Domain-based Message Authentication, Reporting & Conformance (DMARC)

SI.3.220: Utilize email sandboxing to detect or block potentially malicious email attachments

- Technical Requirement
- Establish a sandbox / solution that isolates the execution of attached files or linked URLs
- Protects end user devices and networks from viruses and malware.
- Options May include
  - Hardware based Devices
  - Cloud Services (check for compliance)
  - Server based Solutions

SUMMIT7

Potential Technical Solution Sets

Security Information and Event Management

Coverage for AU.2.044 / AU.3.048 / IR.2.093 / IR.2.094

- SIEM Solutions (SaaS Solutions Not Vetted for FedRAMP or US Persons)
  - LogRhythm
  - LogVault
  - AlienVault
  - Splunk
  - Others

- Summit 7's Preferred Solution
  - Azure Government Sentinel

Backup and Restore

Coverage for RE.2.137 / RE.3.139

- Backup for On Premises and IaaS
  - Dozens of Vendors and Solutions

- Backup for Office 365 GCC High
  - Veeam Backup and Replication
  - AvePoint Office 365 Backup

- Summit 7's Preferred Solutions
  - On Premises and Azure Backup to Azure Government
  - AvePoint Office 365 Backup to Azure Government

SUMMIT7

DNS Filtering

Coverage for SC.3.192

- Potential Solutions (SaaS not vetted for FedRAMP Moderate or US Persons)
  - Webroot
  - Cisco Umbrella (formerly OpenDNS)
  - TitanHQ
  - PaloAlto DNS Security Service
  - ForcePoint

- Summit 7's Preferred Solution

Evaluation In Progress

SUMMIT7

SPAM and Email Protections

Coverage for SI.3.218 / SI.3.219 / SI.3.220

- Potential Solutions (Not vetted for FedRAMP Moderate or US Persons)
  - Cisco Email Security
  - Proofpoint Email Protection
  - Barracuda Spam Firewall
  - FireEye Email Security

- Summit 7's Preferred Solution

Office 365 GCC High Exchange Online P2 / E3 and Advanced Threat Protection Plan 1

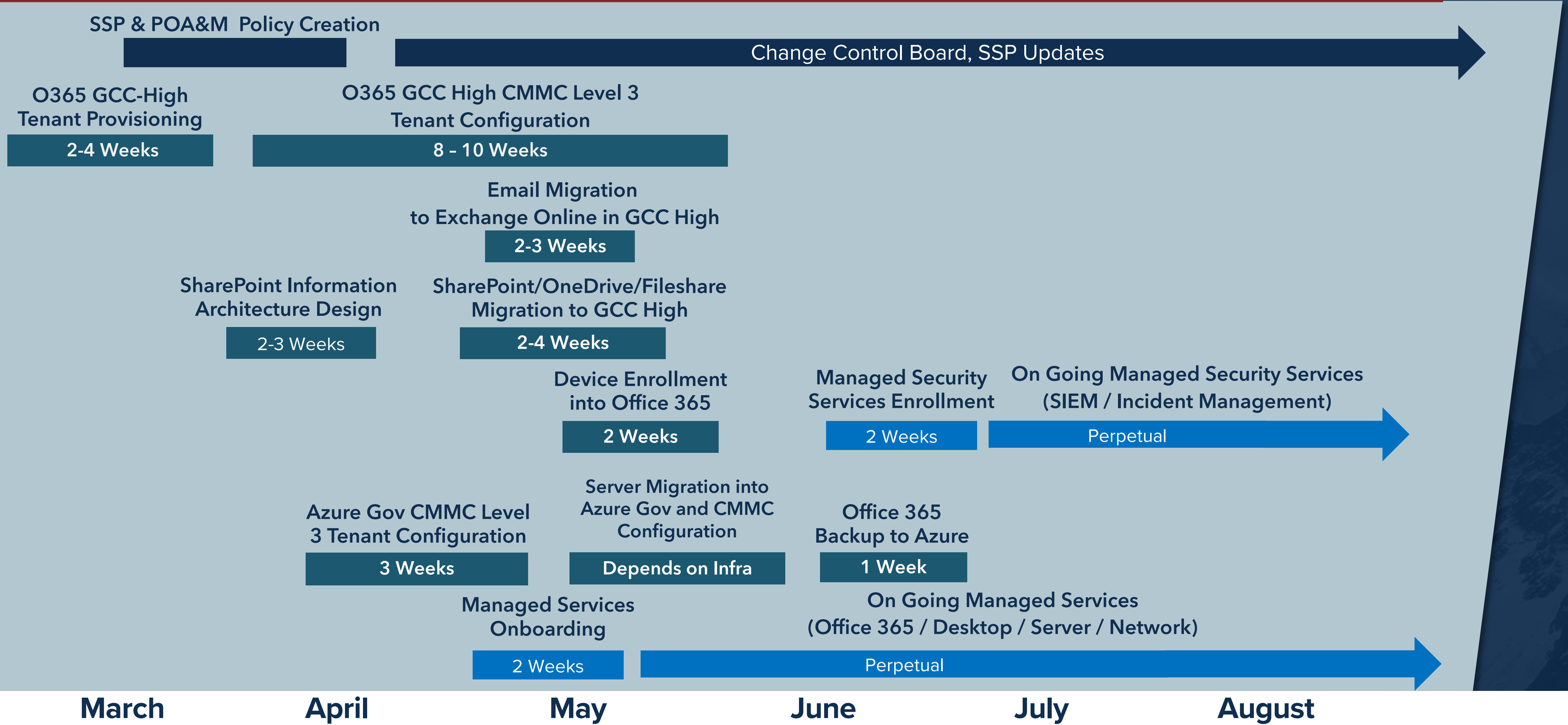
SUMMIT7

What is this going to cost me?!

- What is your current level of readiness?
- Have you (truly) built to NIST 800-171 Already?
- Are you going to build On Premises, Cloud Only or Hybrid Cloud?
- What are the types of costs I may incur?
  - Internal Personnel Costs
    - Initial
    - Perpetual
  - On Premises Hardware / Software
  - Cloud Services
  - 3rd Party Consulting Services
    - Technical Planning and Implementation
    - Procedural Planning and Implementation
  - Managed Services (Desktop / Server / Cloud Management)
  - Managed Security Services (IR / Monitoring / Penetration Testing)

SUMMIT7

Notional Office 365 / Azure Project Roadmap



SSP & POA&M Policy Creation

Change Control Board, SSP Updates

O365 GCC-High Tenant Provisioning

2-4 Weeks

O365 GCC High CMMC Level 3 Tenant Configuration

8 - 10 Weeks

Email Migration to Exchange Online in GCC High

2-3 Weeks

SharePoint Information Architecture Design

2-3 Weeks

SharePoint/OneDrive/Fileshare Migration to GCC High

2-4 Weeks

Device Enrollment into Office 365

2 Weeks

Managed Security Services Enrollment

2 Weeks

On Going Managed Security Services (SIEM / Incident Management)

Perpetual

Azure Gov CMMC Level 3 Tenant Configuration

3 Weeks

Server Migration into Azure Gov and CMMC Configuration

Depends on Infra

Office 365 Backup to Azure

1 Week

Managed Services Onboarding

2 Weeks

On Going Managed Services (Office 365 / Desktop / Server / Network)

Perpetual

March April May June July August

Resources

Blogs: http://cmmc.blog

Videos: http://cmmc.video

Inquiries: cmmc@summit7systems.com