



# HOW TO BUDGET FOR

# • CMMC •

## Understanding the Cost of CMMC Compliance



**Daniel Akridge**  
Director of Engagement  
*Summit 7*



**Sam Stiles**  
VP of Marketing  
*Summit 7*

# HOW TO BUDGET FOR

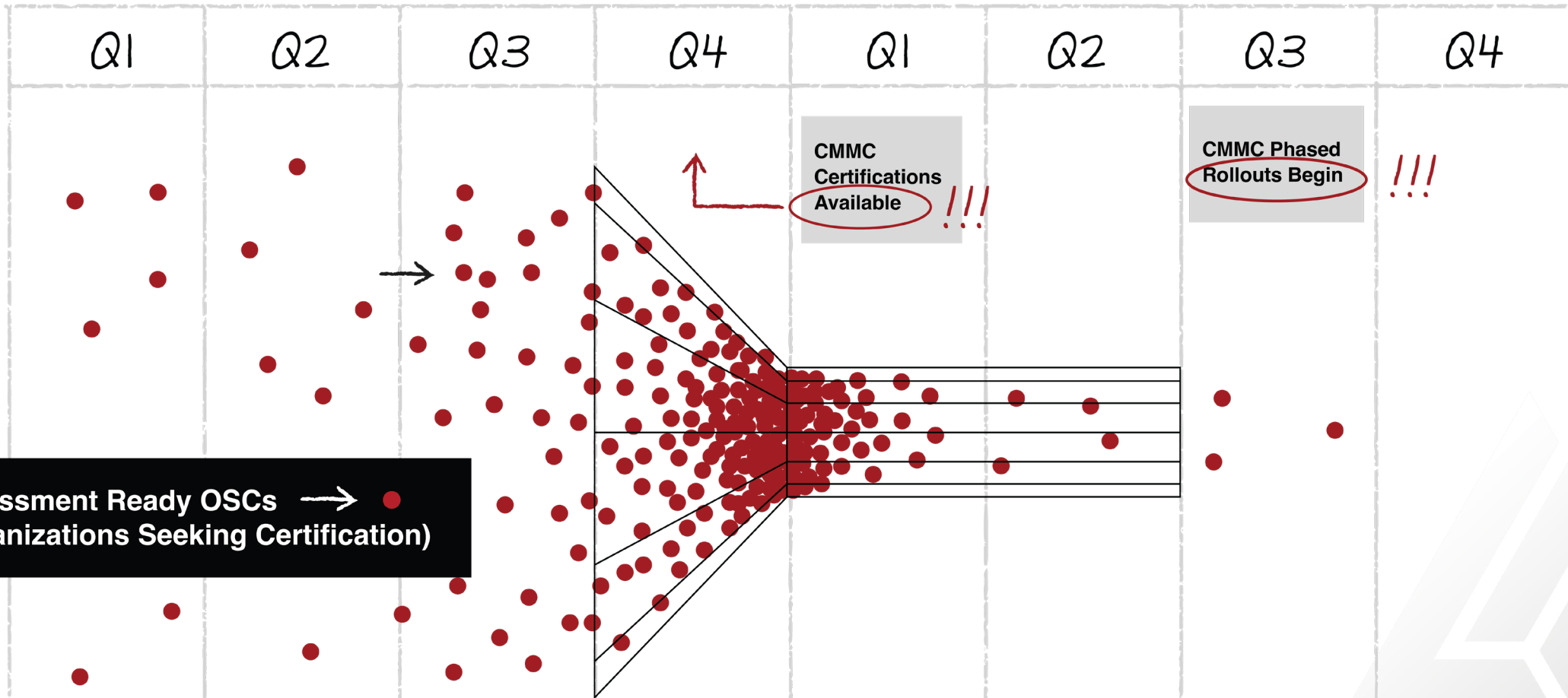
• **CMMC** •

1. **WHAT % OF REVENUE DO I ALLOCATE TOWARDS CMMC?**
2. **WHAT IS THE BEST SOLUTION FOR MY COMPANY?**

# FIRST, WHERE DO WE STAND ON CMMC?

2024

2025

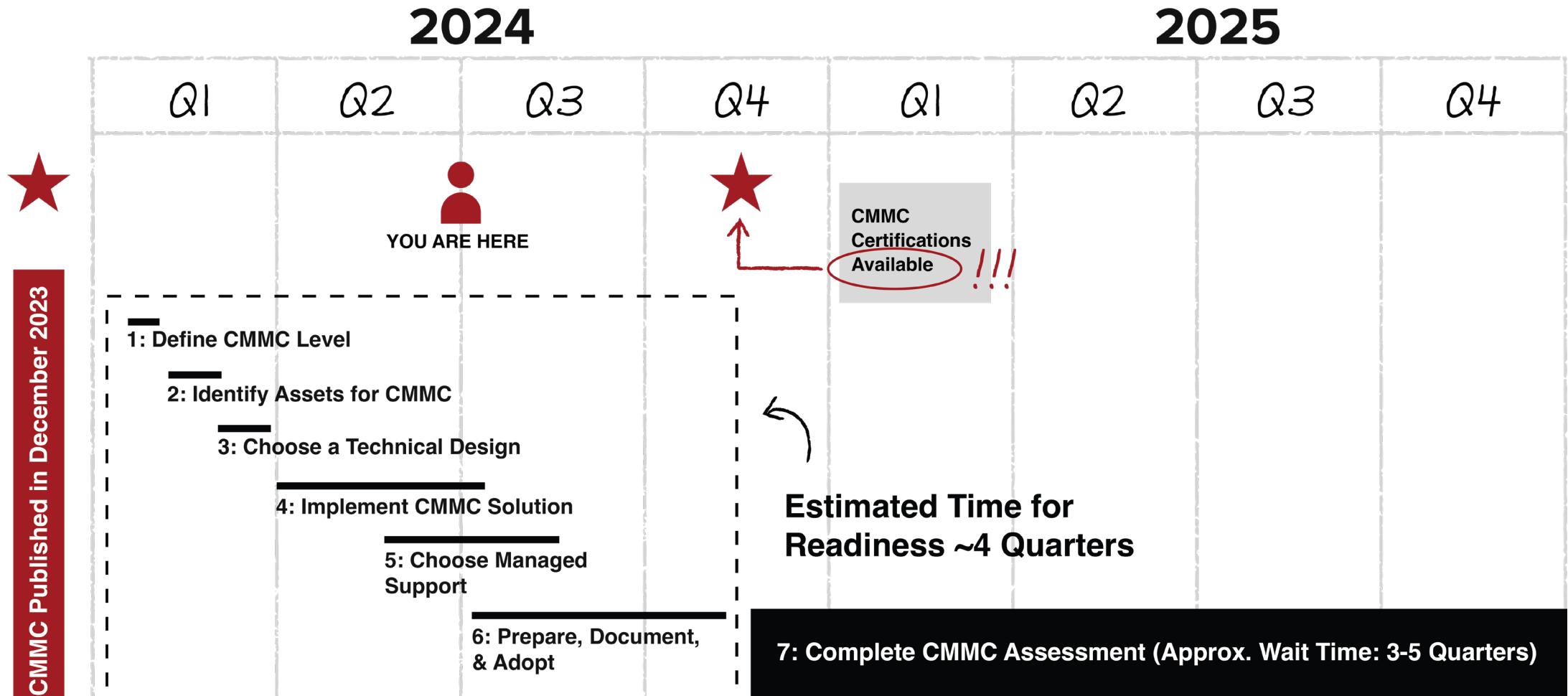


Assessment Ready OSCs →  
(Organizations Seeking Certification)

CMMC  
Certifications  
Available !!!

CMMC Phased  
Rollouts Begin !!!

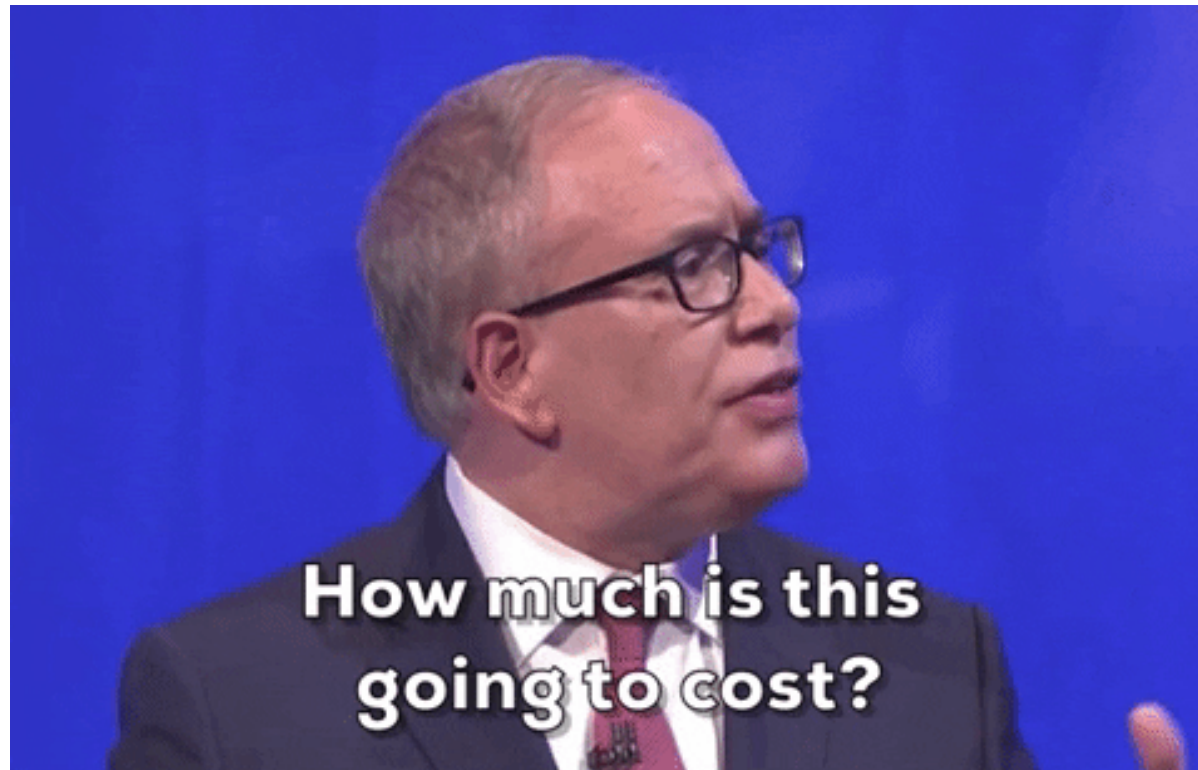
# HOW LONG DOES CMMC TAKE TO DO?



# HOW TO BUDGET FOR CMMC

WEBINAR

THE DIB:



# WHAT DOES THE DOD SAY?

## Revenue Allocation: 0.5%

REVENUE	\$1M	\$5M	\$10M	\$25M	\$50M	\$100M
BUDGET (0.5%)	\$5,000	\$25,000	\$50,000	\$125,000	\$250,000	\$500,000

Based on figures from the Defense Technical Information Center it is estimated that 6,555 contractors would be handling unclassified controlled technical information and therefore affected by this rule. Of the 6,555 contractors it is estimated that less than half of them are small entities. For the affected small entities a reasonable rule of thumb is that information technology security costs are approximately 0.5% of total revenues. Because there are economies of scale when it comes to information security, larger businesses generally pay only a fraction of that amount.

LINK: <https://www.federalregister.gov/documents/2013/11/18/2013-27313/defense-federal-acquisition-regulation-supplement-safeguarding-unclassified-controlled-technical#p-140>

# WHAT DOES THE DOD SAY?

DOD ESTIMATE



## SumITUp EPISODE: Estimating the Cost of NIST SP 800-171

LINK: [https://www.youtube.com/watch?v=DkYefZn\\_wNk](https://www.youtube.com/watch?v=DkYefZn_wNk)

# WHAT DOES THE DOD SAY?

## DOD ESTIMATE

Based on what the DOD published for a NIST 800-53 Implementation we were to calculate what the DOD estimated cost would be for NIST 800-171/CMMC L2.







Cost	Term
\$175,000-\$265,000	One-Time
\$50,000-\$127,000	Annual



# WHAT DOES THE DOD SAY?

## DOD ESTIMATE

If you take the average of both the one-time and annual cost, you end up with \$309,000 in Year 1 spend.

REVENUE	\$1M	\$5M	\$10M	\$25M	\$50M	\$100M
BUDGET (0.5%)	\$5,000	\$25,000	\$50,000	\$125,000	\$250,000	\$500,000
YEAR 1	\$309K	\$309K	\$309K	\$309K	\$309K	\$309K
						

# REGULATED INDUSTRIES

# AVERAGE IT SPENDING

FOR REGULATED INDUSTRIES

Finance	Healthcare	Telecommunications
4.7 – 9.4%	3.0 – 7.0%	5.0 – 10.0%
<ul style="list-style-type: none"><li>• Data Security Standards</li><li>• Cybersecurity Standards</li><li>• Identity &amp; Access</li><li>• Management (IAM)</li><li>• Business Continuity &amp; Disaster Recovery (BCDR)</li><li>• Cloud Computing Regulations</li><li>• Third-Party Risk Management</li></ul>	<ul style="list-style-type: none"><li>• Health Insurance Portability &amp; Accountability Act (HIPPA) Compliance</li><li>• Electronic Health Record (HER) System Compliance</li><li>• Health Information Exchange (HIE) Compliance</li><li>• Meaningful Use (MU) Compliance</li><li>• Data Security &amp; Privacy Regulations</li><li>• Telemedicine &amp; Remote Patient Monitoring Compliance</li><li>• Medical Device Regulations</li></ul>	<ul style="list-style-type: none"><li>• Federal Communications Commission (FCC) Regulations</li><li>• Data Privacy &amp; Security Regulations</li><li>• Network Neutrality Compliance</li><li>• Telecommunications Act Compliance</li><li>• Spectrum Licensing &amp; Management</li><li>• Emergency Communications Compliance</li><li>• Universal Service Fund (USF) Compliance</li></ul>

# AVERAGE IT SPENDING

FOR REGULATED INDUSTRIES

Finance	Healthcare	Telecommunications
4.7 – 9.4%	3.0 – 7.0%	5.0 – 10.0%

## Defense Industrial Base (DIB)

5.0 – 8.0%

- CMMC
- IA PRE
- NNPI
- Export Control

# BUT... WHY SO MUCH?

- **3<sup>rd</sup> Party Certifications**
- **Lack of Expertise  
(Compliance, IT, Cyber)**
- **Compliant Cloud Providers  
& LOB Providers**
- **Compliant Hardware**
- **Supply Chain Cybersecurity Risk**
- **New Regulations/Requirements  
(FAR CUI, CIRCIA, IA PRE)**
- **Managed Service Providers  
Requiring Certification**
- **US Persons and/or Citizens**
- **Additional Internal Time Required to  
Maintain Compliance**

# **GOOD NEWS**

**The whole defense industrial base (DIB) is going to have these requirements.**

**All Products, Goods, Services, etc.... will be expected  
to increase across the supply chain.**

**Simply Meaning: All ships will have to rise with the tide.**

# REGULATED INDUSTRY PERCENTAGES

REVENUE	\$1M	\$5M	\$10M	\$25M	\$50M	\$100M
BUDGET (5%)	\$50,000	\$250,000	\$500,000	\$1.25M	\$2.5M	\$5M
YEAR 1	\$309K	\$309K	\$309K	\$309K	\$309K	\$309K
	✗	✗	✓	✓	✓	✓

# REGULATED INDUSTRY PERCENTAGES

REVENUE	\$1M	\$5M	\$10M	\$25M	\$50M	\$100M
BUDGET (5%)	\$50,000	\$250,000	\$500,000	\$1.25M	\$2.5M	\$5M
YEAR 1	\$309K	\$309K	\$309K	\$309K	\$309K	\$309K



REVENUE	\$1M	\$5M	\$10M	\$25M	\$50M	\$100M
BUDGET (8%)	\$80,000	\$400,000	\$800,000	\$2M	\$4M	\$8M
YEAR 1	\$309K	\$309K	\$309K	\$309K	\$309K	\$309K



IMPORTANT: Proprietary and confidential. Copyright © 2024 Summit 7 Systems, LLC. All rights reserved.





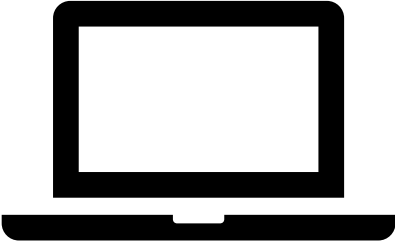
**WAIT, WHAT ABOUT SCOPE?**

**\$309K = ?**

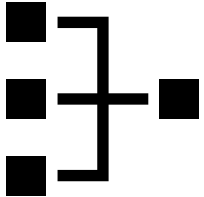
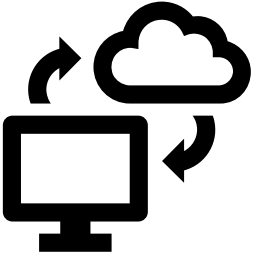
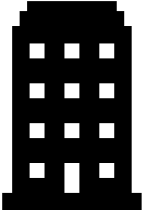
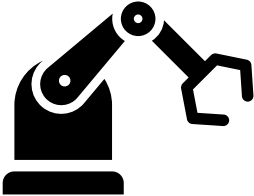
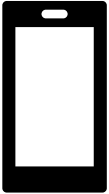
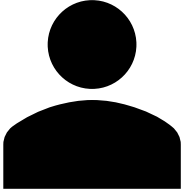
**WAIT, WHAT ABOUT SCOPE?**

**COST = SCOPE**

# WAIT, WHAT ABOUT SCOPE?



## ERP SYSTEM



# WAIT, WHAT ABOUT SCOPE?

## PRO

- CHEAP
- EASY DEPLOYMENT
- BOLT-ON TO EXISTING SOLUTION

## CON

- USER DISCRETION (**HUGE RISK**)
- VERY LIMITED “CUI” COVERAGE
- SUPPLEMENTAL TOOLS NEEDED
- VERY DIFFICULT TO MIGRATE OUT
- CAN'T CONTROL HOW DATA IS RECIEVED

## PRO

- CONTAINED CUI BOUNDARY
- LEAVES CORP OUT OF SCOPE
- EASY TO SCALE/DEPLOY

## CON

- \*CUI DATA FLOW RESTRICTED TO CLOUD
- TWO ENVIRONMENTS TO MANAGE
- CUI ON-PREMISES

## PRO

- SINGLE ENVIRONMENT TO MANAGE
- FULL COMPANY PROTECTION
- CYBERSECURITY INSURANCE
- PROTECTION FROM FUTURE REGULATIONS (**HUGE PRO**)

## CON

- LONG DEPLOYMENT TIME
- EXPENSIVE

## COMPLIANCE RISK METER

FILE SHARING  
TOOLS

VIRTUAL DESKTOP  
CLOUD ENCLAVE

ALL IN  
(WHOLE COMPANY)

# WAIT, WHAT ABOUT SCOPE?

## UNDERSTANDS CUI LOCATIONS

<15% of REVENUE IS DOD (CUI)

<15% of COMPANY IS CUI USERS

## UNSURE OF CUI LOCATIONS

>15% of REVENUE IS DOD (CUI)

>15% of COMPANY IS CUI USERS

## COMPLIANCE RISK METER

VIRTUAL DESKTOP  
CLOUD ENCLAVE

ALL IN  
(WHOLE COMPANY)

IMPORTANT: Proprietary and confidential. Copyright © 2024 Summit 7 Systems, LLC. All rights reserved.



# SO...WHAT DOES IT ALL COST?

50-100 Person Company

## DISCLAIMER:

The costs presented on the next slide are not “Summit 7” prices. This is our effort to paint the full picture of the cost for CMMC compliance.

### List of Items in Cost Estimate

3<sup>rd</sup> Party Assessment (CMMC Certification)

Internal Resources Time

LOB Applications

Microsoft Licensing

Managed Services

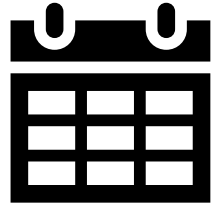
Professional Services

Mock/Gap Assessment

Hardware

# SO...WHAT DOES IT ALL COST?

50-100 Person Company



ONE-TIME

**\$200,000 - \$400,000**

CMMC Implementation  
“All In” or Enclave

Policy & Procedure  
Documentation

Hardware

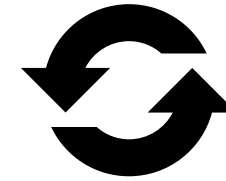
LOB  
Migration

Internal Resource  
Time

Migration of  
Email/Files

Mock/Gap CMMC  
Assessment

Formal CMMC  
Assessment  
(Every 3 Years)



ANNUAL RECURRING - PER USER

**\$400 - \$4,000**

LOB  
Licensing

Hardware  
Refresh

User  
Training

M365 GCCH  
Licensing

Managed  
IT

Managed  
Security

Azure  
Subscription

US  
Support

Managed  
Compliance

# WE KNOW WHY THE DIB HASN'T DONE THIS YET

## JOE'S MACHINE SHOP

Parts + Labor + Compliance = \$10 Per Widget

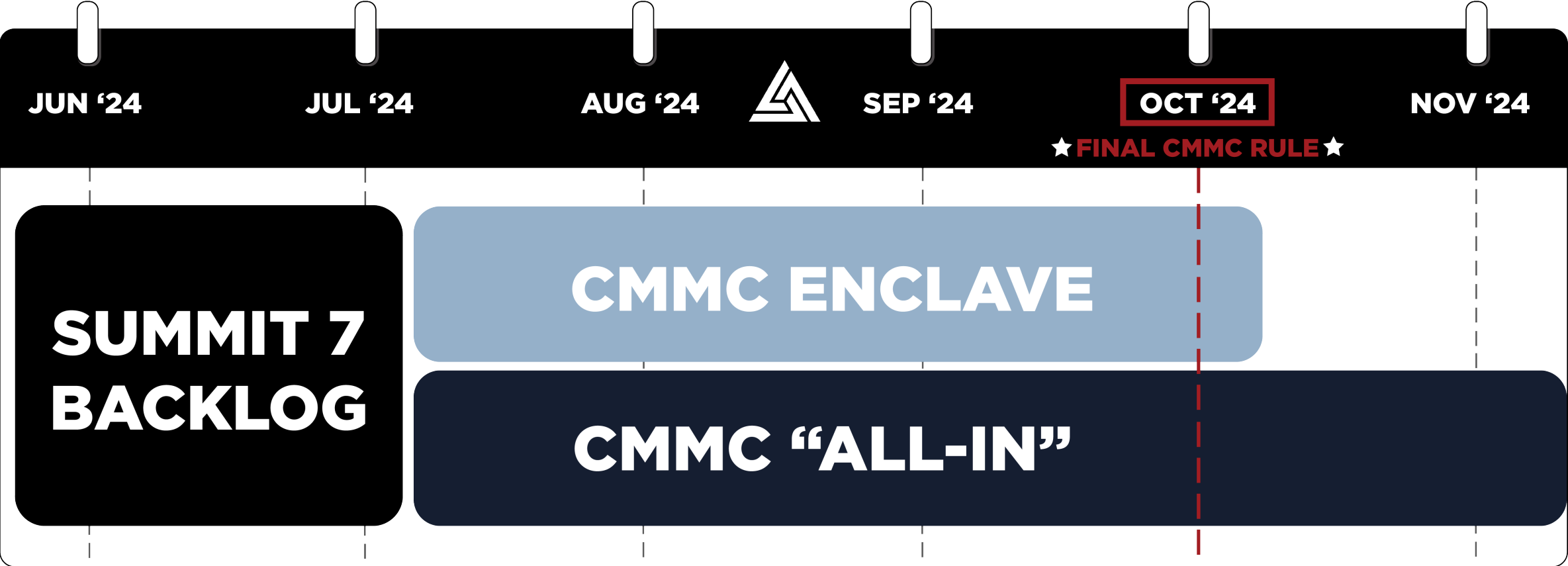
## STEVE'S MACHINE SHOP

Parts + Labor = \$8 Per Widget

Which one does a Lowest Price Technically Acceptable (LPTA) contract select?



# BUT NOW YOU CAN NO LONGER WAIT



# Q&A

FOR MORE INFO CONTACT: [CMMC@SUMMIT7.US](mailto:CMMC@SUMMIT7.US)