PRIME & SUBCONTRACTOR CERTIFICATION

DoD CMMC

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

THIRD-PARTY CERTIFICATION (MANDATORY)
100% OF THE DoD SUPPLY CHAIN (NO EXCEPTIONS)

RubinBrown®

202-679-5100 | rubinbrown.com

Presentation Team

Mike Drevline

National Practice Leader, Aerospace & Defense Industries

U.S. Army Special Forces, Special Operations Command & Intelligence Community Veteran

Rob Rudloff (CISSP, ISSMP)

Global Director of Cybersecurity

U.S. Air Force, Pentagon & Intelligence Community Veteran

Mark Clark (CISSP, CPA, CEH)

Senior Compliance & Cybersecurity Team Leader

U.S. Marine Corps Force Reconnaissance Team Leader, U.S. Embassy Security Specialist

Michael Shapow

Consulting Practice Leader (Chicago)

RubinBrown

OVERVIEW | DoD CMMC

- DoD Created Cybersecurity Maturity Model Certification (CMMC)
- Certification is Mandatory to Bid & Perform on All Contracts
- Contracts & Agencies Served will Specify Level Required (L1-L5)
- Majority of Controls from NIST 800-171 (110 Controls)
- Prime & Subcontractors Certified Separately
- 350,000+ will become Certified (Entire DoD Supply Chain)
- Limited Certifiers to Contractors Ratio Will Create Huge Backlog

RubinBrown

DoD CMMC Timeline

JANUARY
31

DoD CMMC Launched (v1.0, Currently v1.02)

All Contractors, Prime & Subcontractors

NOVEMBER
30

RFIs - Inquiries Begin, RFPs to Follow

Remediation & Trial Certification Completed

11/30
DFARS

DFARS Interim Rule for Contract Holders

Increased Fines for Non-Compliant Primes & Subcontractors

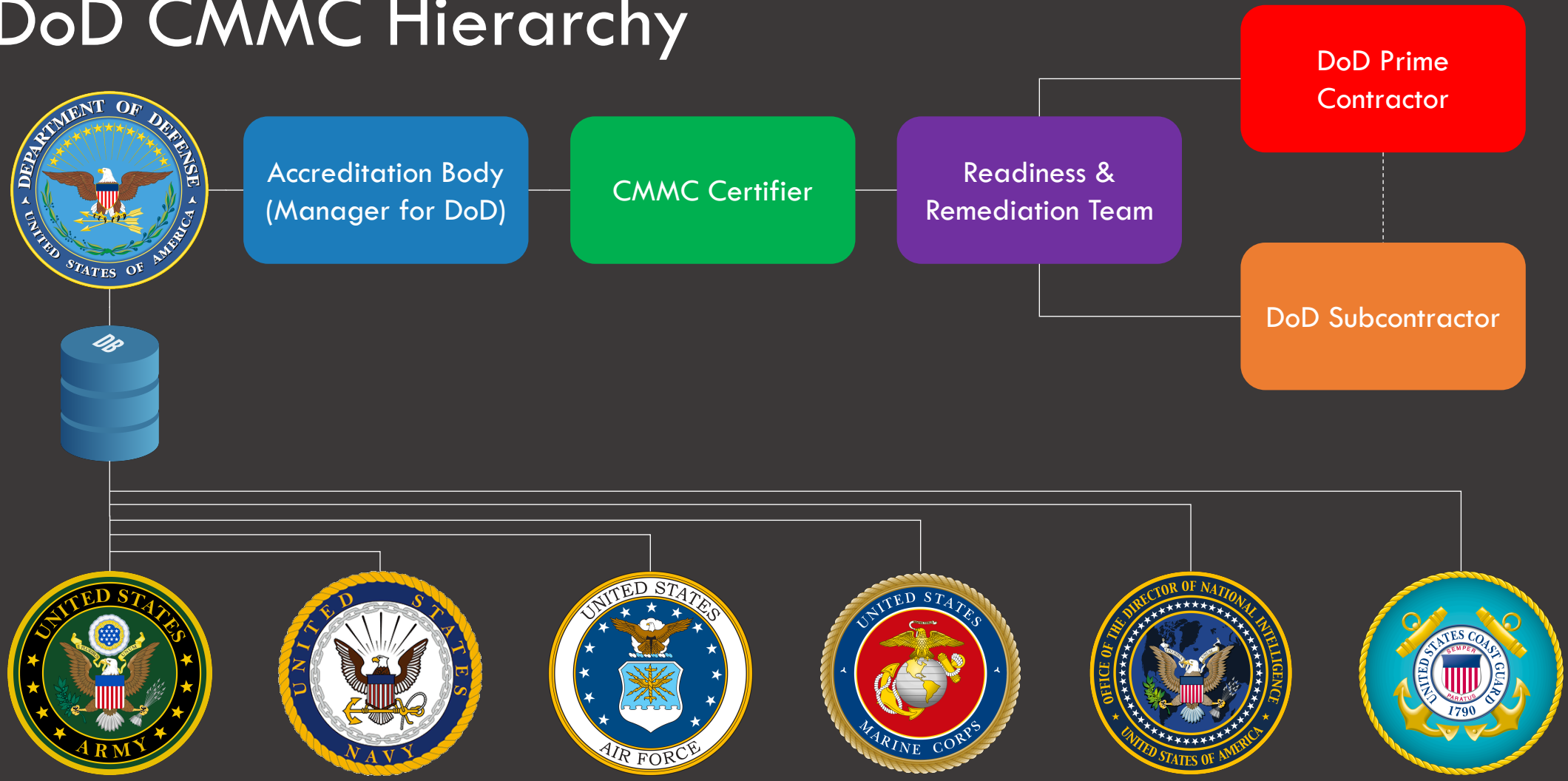
RubinBrown

What is the DFARS requirement for 11/30?

- 100% of DoD contractors by 11/30 are required to self-assess, known as a "Basic Assessment", under the NIST 800-171 framework, to the SPRS/PIEE Web Sites
  - DoD performs Medium & High Assessments
- DFARS interim rule attempts to bridge the initial self-assessment requirement and the upcoming CMMC process
- Is your basic assessment/self-assessment accurate?
  - Grand majority of self-assessments our team reviewed were inaccurate, incomplete, or failed to meet requirements

RubinBrown

DoD CMMC Hierarchy



DoD CMMC Hierarchy

Today

Tomorrow

& Many Others

DoD CMMC SERVICES

READINESS ASSESSMENT
REMEDIATION
PRE-CERTIFICATION AUDIT
TRANSFER TO CERTIFIER

PERFORM CERTIFICATION (L1-L5)
REVIEW WITH DOD CONTRACTOR
CMMC SUBMITTAL

CERTIFICATION REVIEW
ON-SITE/OFF-SITE SECURITY REVIEW (SOC)

RubinBrown

DURATION OF EACH STAGE

- Pre-Certification
  - Assessment (~4-weeks, depending on # of locations)
  - Remediation (3 to 6-Months)
    - A number of factors dictate the length of remediation including the number of locations, number of personnel, complexity of systems. We provide a detailed roadmap and timeline with our assessment.
- Certification (TBD)
  - Includes both On-Site and Off-Site Time
- Post-Certification

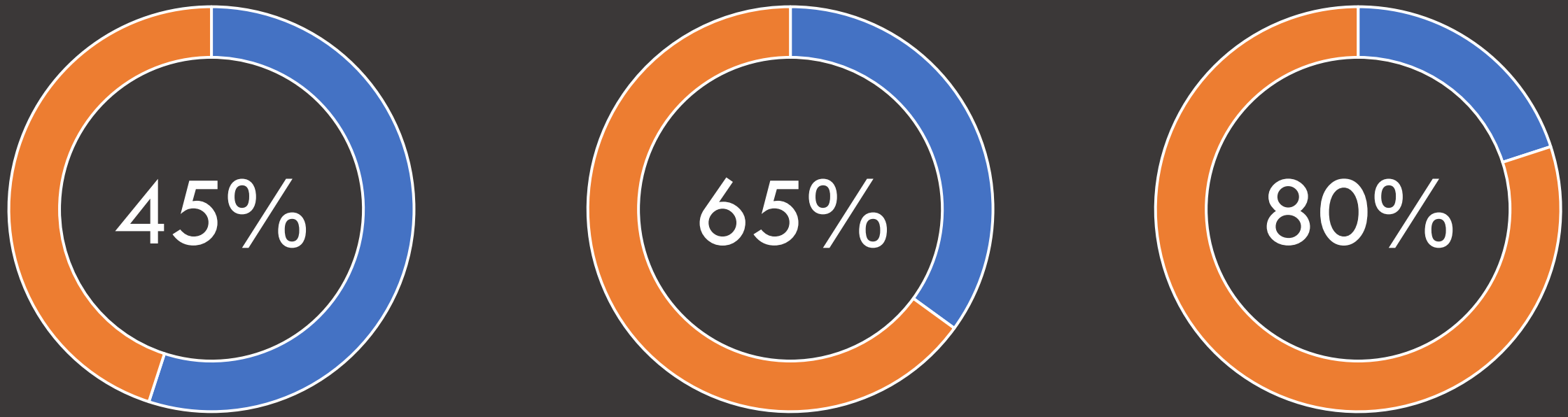
RubinBrown

COSTS (Based on CMMC Level 3 Certification)

- Readiness Assessments
  - $15K to $30K
- Remediation
  - 3 to 5x Cost of Assessment (varies based on compliance requirements)
- Certification
  - Cost TBD (DoD discussing with market, B2B transaction)
  - DoD Discussing Reimbursing Contractor for Certification Cost
- Post Certification (Based on Complexity of Organization)

RubinBrown

CMMC FAILURE RATE



STEP 1 | READINESS ASSESSMENT

- Review of Operation
  - Technology
    - Software/Hardware (all environments)
  - Human Capital
    - Training Process, Competency Levels
  - Policy & Procedure
    - Industry-Specific, Government Requirements
- Security Lead and/or Team Assessment
- Creation of Road Map for Remediation

RubinBrown

STEP 1 | ASSESSMENT DELIVERABLES

- Readiness Assessment Deliverable
  - Detailed Executive Summary Highlighting Areas “Not Implemented”
  - DoD CMMC Readiness Report (all controls, implemented or not)
  - NIST 800-171 Readiness & Compliance Report
    - System Security Plan (SSP) Included
    - Plan of Actions with Milestones (POA&M) Included
  - Roadmap to Remediation
    - Define the process to perform the remediation yourself, with an external team (RubinBrown) and/or others
    - Define typical hours to implement control(s)

RubinBrown

STEP 2 | REMEDIATION

- Implement Plan of Action & Milestones (POA&M)
  - Identify needed resources
  - Identify timeline
  - Implement "easy" controls first (quick wins)
  - Get executive "buy in"
  - Prepare users for changes if needed (MFA, training)
  - Track progress in POA&M
- Create/Update System Security Plan (SSP) & POA&M

RubinBrown

STEP 2 | REMEDIATION (Continued)

- Refinement
  - Updating/Adjustment of Existing Systems
  - Configuration of Key Protection Systems
  - Construction of Training Materials & Sessions
- Integration & Implementation
  - Cloud Implementation (Microsoft Azure, IBM, AWS)
    - Office Tools, Storage, Intranet/Extranet
  - Security Systems (Software/Hardware/Cloud)
  - ERP Implementation (Accounting & Finance, HR)

RubinBrown

MULTI-REPORT | COMBAT MULTIPLIER

RubinBrown

STEP 3 | CERTIFICATION

- Perform Certification (L1-L5)
- Review with DoD Contractor
- Preparation for Submittal
- CMMC Submittal to DoD Accreditation Body
- CMMC Accreditation Body Review
  - Go/No-Go
- DoD/Certifier provide Certification #/Certificate
- Communicate Renewal Date

RubinBrown

STEP 4 | POST-CERTIFICATION

- Certification Review
  - Reviewing point-in-time setup/operations against most recent CMMC
- Assessment/Remediation Review
  - Reviewing most recent findings of internal and external IT initiatives
- Pre-Certification Advising & Support
- Roadmap for Remediation
- On-Site/Off-Site Security-as-a-Service (SOC)
- Staff/Executive Training

RubinBrown

Q & A

- What CMMC level are we required to be certified?
- Who performs it?
- Do my subcontractors need to be certified?
- Is it worth remediating open issues internally?
- How long does remediation take and at what cost?
- Can I bid/participate without being certified?
- What's the cost of the certification?
- How long does my certification last?
- What happens if I'm a "no-go" for my certification?

CONTACT INFORMATION

- Mike Drevline, National Practice Leader (U.S. Army & Intelligence Community)
  - mike.drevline@rubinbrown.com or 202-679-5100
- Rob Rudloff, Director of Cybersecurity (U.S. Air Force & Intelligence Community)
  - rob.rudloff@rubinbrown.com or 303-590-8770
- Michael Shapow, Partner
  - michael.shapow@rubinbrown.com or 312-805-1554
- Mark Clark, Senior Team Leader (U.S. Marine Corps)
  - mark.clark@rubinbrown.com or 618-363-5240

RubinBrown

Important Web Sites

- Supplier Performance Risk Assessment (SPRS)
  - https://www.sprs.csd.disa.mil/
- Procurement Integrated Enterprise Environment (PIEE)
  - https://piee.eb.mil/piee-landing
- DoD CMMC
  - https://www.acq.osd.mil/cmmc
- RubinBrown DoD CMMC
  - https://www.rubinbrown.com/Services/business-advisory-services/Cyber%20Security/cybersecurity-maturity-model-certification.aspx

RubinBrown