

ROADMAP TO CMMC

6 MONITOR CYBER RISK MATURITY

- Continual awareness of your CR Posture
- Key Business Drivers:
 1. Board Reporting
 2. CR Insurance
 3. M&A Valuation Discriminator
 4. Business Impacts of Non-Compliance
 5. Brand & Reputation

5 OPERATIONALIZE YOUR CR MANAGEMENT

- Continuous Assessment, Reporting, and Remediation
- Generate evidence to demonstrate increasing maturity
- Employ robust employee cybersecurity awareness training
- Don't forget your supply-chain!

1 DEFINE CYBER RISK (CR) AS A KEY BUSINESS ENABLER

- Understand total base of Federal work
- Define strategic growth planning 2-5 years out
- Account for "Cyber Cost" of doing business (OH, ODCs, Supply Chain, etc.)
- Corporate Backing critical to affect culture change

2 FORM (CR) TEAM

- Designate a senior member as CR Officer to lead initiative
- Assemble key members (IT, DevOps, Contracts, Legal)
- Identify 3rd Party Service Providers (TSPs)
- Understand FAR & DFARS cyber requirements
- Consider consult with a CR Advisor

3 ASSESS YOUR FCI/CUI DOMAIN

- Know where data lives across your IT landscape
- Identify opportunities to reduce exposure
- Account for data flows in your Supply Chain and TSPs

4 KNOW YOUR CYBER RISK POSTURE

- Confirm your compliance objective (e.g., NIST 800-171, CMMC L3)
- Assess your Readiness
- Develop plan to address gaps
- Start moving towards compliance