Project Explanation: I created this roadmap and the web page recommendation based on the needs of a business to help customers understand new government requirements. Their target audience was small and mid-sized businesses who may or may not know about CMMC. The topic is large and can be difficult to understand, so I created the below document to help which compliments the clients services.

DoD Contractor's CMMC Roadmap

A checklist to follow on your journey to be CMMC certified!

Take it One-Step-at-a-Time

The multiple recent cyberattacks are overwhelming evidence that America is overdue for a cyber security over-hall. If you are a DIB (Defense Industry Base) supplier, direct DoD contractor or even a DoD subcontractor then it is time to up your security game.

According to the *US Federal Government, "it is estimated that 129,810 unique entities will pursue their initial CMMC certification during the initial five-year period. By October 1, 2025, all entities receiving DoD contracts and orders, other than contracts or orders exclusively for commercially available off-the-shelf items or those valued at or below the micro-purchase threshold, will be required to have the CMMC." **Federal Register / Vol. 85, No. 189 / Tuesday, September 29, 2020 / Rules and Regulations*

CMMC certifications are valid for three years. Therefore, large, and small businesses will be required to renew their certification every three years. For every unique prime contractor (about 220,000), there are approximately 100 unique subcontractors. CPI Systems has created a roadmap so you can easily be ahead of the crowd on your CMMC Certification journey.

Checklist for your CMMC Certification Journey

Secure Your Knowledge Base

- Determine if your company handles any FCI (Federal Contract Information) or CUI (Controlled Unclassified Information). There are 24 categories and 83 subcategories of CUI content.

- Know the business case for CMMC Certification. Manufacturing Extension Partners (MEP's) may help small businesses with funding.
- Explore if you need the entire company to be CMMC certified, or only a specific division of your company.
- Assess your CMMC in-house expertise and bandwidth and determine where you need help navigating most.
- Read up on all things CMMC and/or Contact CPI Systems workshop(s) to bring you up to speed. *(insert Workshop page link here)*
- Determine if you need Level 1 or Level 3 certification; or get a FREE Consultation from CPI Systems.

Project Plan with the Right Partners

- Set a timeline for obtaining CMMC Certification(s).
- Select your RPO (Registered Provider Organization). CPI Systems is an RPO and ideal choice for SMBs in the electronics, fabricating, and manufacturing sectors.

NIST-SP 800-171 Basic Self-Assessment and Scoring

- Read through the 110 published NIST-SP 800-171 standards including Domains, Processes, Capabilities, and Practices.
- Do an informal gap analysis determining where your largest needs are to get to compliance. Begin business discussions and get connected with resources. CPI Systems can help!
- Perform a NIST-SP 800-171 Basic Self-Assessment *(insert page link here)* on all storage, processing and transmitting of DoD related information as related to the 110 published standards.
- Hire an Authorized Provisional Assessor to score the NIST-SP 800-171 Self-Assessment. *(insert page link here)*

Post Your Assessment Results in SPRS (Supplier Performance Risk System)

- Keep your results current, within three years or less.
- Provide the DoD with visibility into the scores you have completed and if you are at Basic, Medium, or High and have the security needed for the DoD contract under negotiation.

Document Gap Analysis, SSP (System Security Plan) and POAM (Plan of Action & Milestones)

- Complete a formal Gap Analysis through building a bridge from where you are to where you need to be.
- Create the SSP outlining how your organization implements security DAFRS (Defense Acquisition Regulation Supplement) Requirements.
- Outline the plan of action and significant milestones to reach along the way. (POAM)
- Keep clear and detailed documents for each step or hire someone to do this for you.

Complete Level 1 Certification

- Train applicable employees on Level 1 CMMC Certification.
- Secure an Accredited C3PAO (CMMC Third Party Assessment Organization). CPI Systems can facilitate an ideal assessor for your organization.
- Secure any new information technology systems vendors needed to comply with your computer hardware and software security for CMMC Level 1 Certification.
- Create a clear document containing all policies, practices and objective evidence that relate to CMMC Certification.

Complete Level 3 Certification

- Train applicable employees on Level 3 CMMC Certification.
- Complete the 20 additional CMMC Practices required in addition to the 110 NIST 800-171 requirements for Level 1 Certification.
- Secure an Accredited C3PAO (CMMC Third Party Assessment Organization). CPI Systems can facilitate an ideal assessor for your organization.
- Secure any new information technology systems vendors needed to comply with your computer hardware and software security for CMMC Level 3 Certification.
- Update your Level 1 document to contain all policies, practices and objective evidence that relate to CMMC Level 3 Certification.

Maintain Certification

- Create a system whereby all actions related to the CMMC standards are checked for compliance regularly.
- Keep up-to-date on all ongoing documentation regarding CMMC Certification maintenance.
- Appoint an employee to serve as compliance manager or hire CPI Systems for Compliance Management as a Service CMaaS℠.

Contact Us about Your CMMC Needs

(should be a CTA (call to action) button)