WHAT DOES MY BUSINESS NEED TO DO?

If your company is in the Department of Defense (DoD) supply chain, you will be required to hold Cybersecurity Maturity Model Certification (CMMC**).** CMMC is a quality management system/maturity model designed to minimize/mitigate cybersecurity risks, so compliance is a business function and requires an integrated approach between owners, managers and IT. The level of certification (Levels 1 – 5) depends on the types of data you process and/or create – Controlled Unclassified Information (CUI) or Federal Contract Information (FCI).

The DoD estimates that 85% of the Defense Industrial Base will need to be certified to CMMC Level 1; therefore, the Interagency Cybersecurity Coordinating Committee's mission with regard to CMMC is to assist companies with Level 1 certification by providing information and resources.

Depending on the complexity of your organization and/or your IT system, you may need to engage a consulting company to assist you with compliance. ***NOTE: Consulting companies cannot promise that they can get your company certified to CMMC, and certification to NIST 800-171 does not exist. The most they can do is work with the standard as it is currently written and help your company with compliance.***

Step 1

1) Read the What is CMMC? section
2) Review the CMMC Overview presentation
3) Listen to CMMC Accreditation Body Conversations (multiple conversations)
4) Read the CMMC FAQs

If you are currently a DoD contractor, please proceed to Step 2.

If you are not a DoD contractor, but are interested in entering the DoD market, begin by reviewing the CMMC Level 1 Requirements ***presentation.***

Step 2

Review your current contract to see if the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 is referenced. This applies to subcontractors as well – the DFARS clause may be flowed down to you. If it is, the contracting officer anticipates that you will be processing or creating Controlled Unclassified Information (CUI). By accepting the award, you have implicitly self-attested that your company is compliant to National Institute of Standards Special Publication 800 – 171, which governs CUI in Non-Federal Information Systems and

Organizations. If you are concerned about compliance to the DFARS clause, you need to refer to CMMC Level 3 requirements (CMMC Level 3 maps closely to NIST SP 800-171) to see if your company has the appropriate practices/controls in place. Resources: CMMC Model; CMMC Appendix - Requirements in Table Format; Project Spectrum is a DoD-supported source of information for small businesses to use to help with CMMC compliance

If **DFARS 252.204-7012** is NOT referenced, you will not be processing or creating CUI. You are most likely processing and/or creating **FCI.** You should begin the process of becoming compliant to CMMC Level 1.

Step 3

Prime contractors need to look at the types of data you currently share with your suppliers and subcontractors (subs). **CMMC requirements follow the data, so you may not need to flow down CMMC requirements to your subs and suppliers**. Once you have determined whether your subs/suppliers will be processing CUI or FCI, you should work with them on the appropriate CMMC certification level. It is critical for national security that our supply chains remain intact, and DoD expects prime contractors to do their part to help the companies in their supply chains with CMMC.