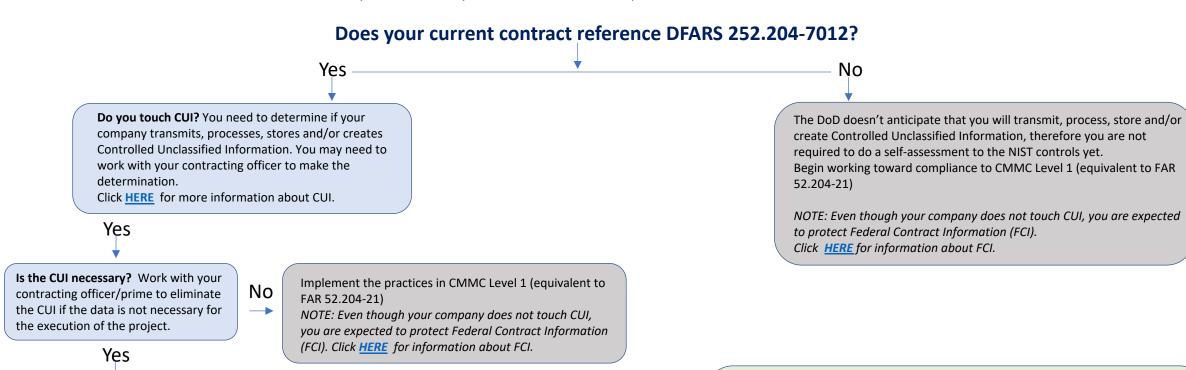
Decision Tree: DFARS or CMMC

Department of Defense cybersecurity regulations do not apply to companies that supply Commercial-Off-The-Shelf (COTS) products or sell products below the micro-purchase threshold to the DoD.



The DFARS Interim Rule applies. Click <u>HERE</u> to access information and tools to assist with your self-

Yes

After you complete the tasks required by the new DFARS Interim Rule, consider working toward compliance to CMMC2.0 Level 2.

Determining if your company touches CUI or not is the most important thing to consider in developing a cybersecurity program, in terms of risk and cost. See below.

Touching CUI requires the implementation of 110 NIST controls, a self-assessment to those controls, and uploading your score to SPRS..

It is in your company's best interest AND in the best interest of national security to avoid touching CUI.



assessment.

While this document is deemed a public record by North Carolina law, the North Carolina Military Business Center owns the copyright to this document. With attribution to NCMBC, the NCMBC provides a non-exclusive, royalty-free, perpetual license to copy and distribute this document

Decision Tree Notes

- Remember if your contract references DFARS 252.204-7012 that doesn't necessarily mean that you touch CUI. **The clause is only applicable if you touch CUI. NOTE:** Prime contractors often require a higher level of compliance from their subs and suppliers than is necessary. Try to work with them to only flow down requirements and data that are necessary to perform the work.
- All the cybersecurity regulations are based on the protection of DoD data FCI or CUI. To know which
 regulation your company must comply with, it is critical that you know what type(s) of data the
 contracts require you to transmit, process, store and/or create.
- If your company touches CUI, you must comply with DFARs clauses 252.204-7012/7019/7020, which means you should begin implementing the 110 controls in NIST SP 800-171 AND comply with every requirement in the three clauses.
- If your company only touches FCI, you must comply with FAR 52.204-21, which means you should begin implementing the 17 controls in CMMC 2.0 Level 1.

CUI = \$\$\$ + Risk AVOID IT IF POSSIBLE!