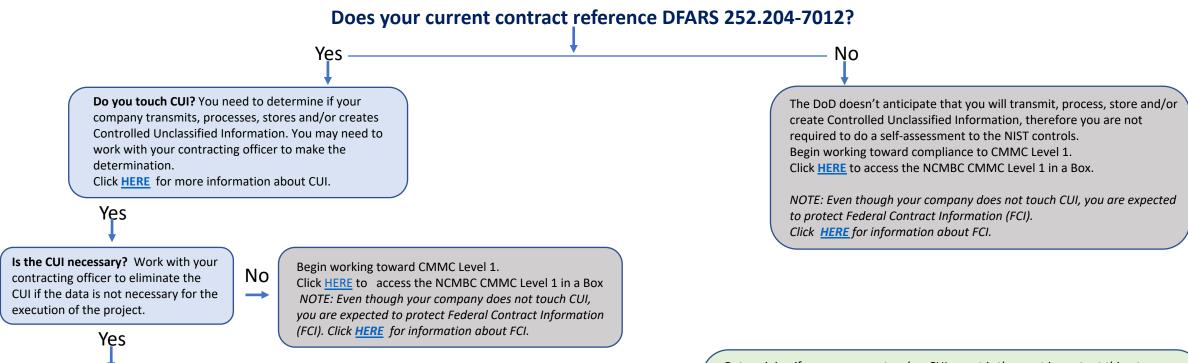
## **Decision Tree: DFARS or CMMC**

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-assessment.

Yes

After you complete the tasks required by the new DFARS Interim Rule, begin working toward compliance to CMMC Level 3. Click HERE 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 plus the additional 20 controls required by CMMC Level 3 - which for some companies can be cost-prohibitive. The cost of an audit alone can be in excess of \$30K.

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



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.
- 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 or create.
- CUI means compliance with the DFARS clause, and that means compliance with the 110 controls in NIST SP 800-171. CUI also means that eventually you will be required to comply with CMMC Level 3, which is a cybersecurity program which adds 20 additional controls to the 110 NIST controls.
- FCI means compliance with FAR 52.204-21, which means you must comply with the 17 controls in CMMC Level 1.

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