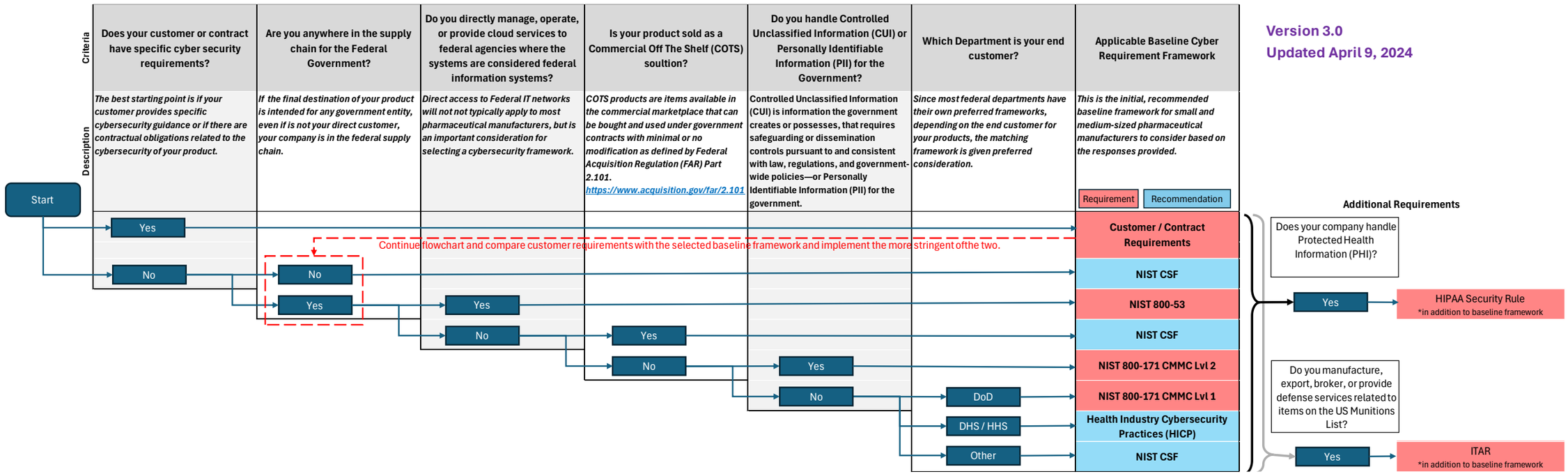

Version 3.0
Updated April 9, 2024

NOTES

- **Guidance, Not Prescription:** This flow chart serves as a guide rather than a definitive or authoritative resource. It aims to facilitate discussion with companies to help them navigate towards the appropriate cybersecurity framework. Each framework comes with its own set of advantages and limitations, and ultimately, the decision on which to adopt rests with the company.
- **Starting Point - Customer Requirements:** The journey begins with the specific requirements provided by the direct customer. Engaging in dialogue with the customer about cybersecurity expectations is crucial. Even if customer-specific guidance exists, companies are encouraged to proceed through the flow chart (as indicated by the dashed return line) and adopt more stringent measures between the customer's guidelines and the identified baseline framework.
- **Stay Updated:** The regulatory environment for cybersecurity is ever evolving. While this tool is a valuable starting point, it is important to check with cybersecurity requirements experts and utilize the latest version of whichever framework is selected to ensure compliance with current standards.
- **Additional Requirements - ITAR and HIPAA:** ITAR and HIPAA requirements possess unique considerations and should be treated as supplementary to any other baseline framework selected by the flow chart. They add an additional layer of complexity and specificity to the cybersecurity measures that a company must undertake.
- **Hard Requirements vs. Recommendations:** It's important to recognize that some frameworks entail hard requirements—such as CMMC for DoD contractors—while others might offer recommendations. This distinction is visually represented in the flow chart using blue (for recommendations) and red (for hard requirements) colors, aiding in the understanding of each framework's nature and obligatory level.

Recommend Require