1. OVERVIEW

The Government has frightened contractors, especially small businesses, by announcing that without Cyber Maturity Model Certification (CMMC), a company cannot be considered for a Government contract. The trouble is, very few people can accurately answer what being CMMC certified (yes, a technically redundant term) means, let alone translate it into return on investment (ROI) terms. If CMMC compliance costs a company $100,000 to keep a Government contract that yields a profit of $10,000, why should the company pursue CMMC? The only way to know is to do the difficult work of determining solid estimates for cost-benefit analyses. SandTech had to figure this out for itself. We then applied the (hard) lessons learned to other companies to present them with cost-benefit analyses. As soon as we lay out the figures, the business case (pro or con, depending on the company) is clear.

2. "WE WANT CMMC – WHATEVER THAT IS. . ."

What is CMMC?

CMMC is a Federal program to ensure its Controlled Unclassified Information (CUI) is protected. CUI is "any information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls," but does not include certain classified information. Federal Contract Information (FCI) is "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government." It does not include public information or certain transactional information. CUI is a subset of FCI since you cannot share FCI information, but you must proactively safeguard CUI.

First, let us make sure we understand the Government's perspective.

[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible]

- [illegible]