Heads up, defense subcontractors: Just because your prime contractor is CMMC-compliant doesn't mean you are

AUGUST 13, 2020BY RISA SAVOLD

While the Cybersecurity Maturity Model Certification (CMMC) is about to make a substantial impact on all defense suppliers, this conversation is really for the defense subcontractors out there. We have some bad news: your prime contractors may not be much help when it comes to proving CMMC-compliance.

A quick update on the CMMC timeline

The draft rule DFARS 252.204-7012—which requires all defense contractors to achieve Cybersecurity Maturity Model Certification (CMMC)--is still reported to be on track. The U.S. Department of Defense (DoD) is expected to release the draft for public comment soon.

We don't know for certain what "soon" means, but we do know what the DFARS rulemaking process looks like once the rule is released to the public. Here are the timeframes defense contractors can expect.

- **60 days.** Industry and other stakeholders can participate in a public hearing and 60-day comment period to give feedback on the proposed DFARS rule language.
- **After 60 days.** The updated DFARS rule, with public commentary considerations incorporated, is published.
- **30 days.** The new DFARS regulation goes into effect 30 days after the publish date.

Despite being at least 90 days away, prime contractors aren't waiting around for the final word on the new DFARS regulation. Per the expected requirements in DFARS 252.204-7012 and the contract flowdown clause, **all** defense suppliers will need to maintain their **own** CMMC certification level.

Prime contractors are conducting due diligence now

Since each supplier will need to maintain their own CMMC certification level, prime contractors are now starting to survey their own supplier communities to understand each supplier's certification status, sometimes with requested responses required within 30-60 days. Here are some of the questions being asked:

1. Have you conducted a self-assessment of your company's compliance with CMMC?
   If yes, at which CMMC level are you compliant with today?
2. Have you had a third party perform a CMMC assessment of your company?
   If yes, at which CMMC level did they find you compliant today?
3. At which CMMC level do you currently plan to be certified?
4. What is your current target date to obtain CMMC certification at that level?
5. Are there any specific CMMC requirements that you have determined will not be feasible for your company to achieve?
6. Do you have any remaining POA&Ms to resolve compliance issues with NIST SP 800-171 requirements?
7. Do you have a clear understanding of what is considered Controlled Unclassified Information (CUI) and where you store, process, or transmit CUI today, if applicable?
8. Are you staying current and informed of the status of the CMMC regulation?
9. What steps have you taken, or plan to take, to assess whether your suppliers are ready and able to achieve the necessary CMMC certification?

For prime contractors, questionnaires like this are part of their risk management efforts to identify the readiness of their critical supply chain and avoid disruptions to their business.

Prime contractors have a few options if they want to continue working with suppliers that will not receive CMMC in time or do not plan to achieve CMMC on their own. For example, prime contractors can 1)

provide working space for subcontractors in their own secure facilities; or 2) they can issue pre-configured, secure laptops for subcontractor use.

Both these options are common in federal contracting. However, these approaches can result in sizable direct costs for prime contractors due to the purchase of additional IT equipment, as well as the additional asset, personnel, and facilities management.

Prime contractors are likely to carefully identify which subcontractors they share CUI with, and then use this information to determine their critical, sole-source suppliers. Of all the suppliers in the prime contractor's ecosystem, the sole-source suppliers with shared CUI may be best positioned to receive additional support to still participate in RFPs despite not having CMMC compliance.

Subcontractors cannot assume the CMMC level of their prime contractor

For previous RFPs, defense subcontractors that didn't have direct government contracts or respond directly to RFPs were often under the radar. Even with the contract flowdown clause, prime contractors may or may not have requested the System Security Plans of all their suppliers or verified compliance with NIST SP 800-171. The combination of the new certification with the contract flowdown clause now means that the defense industrial base will face much closer scrutiny.

While we've said this previously, it bears repeating: when it comes to CMMC, subcontractors cannot assume the CMMC level of their prime contractor. Subcontractors also cannot assume the prime contractor will provide additional support to accommodate their non-compliance.

This is where the subcontractor CMMC surveys come in. Prime contractors could use the information gleaned from these surveys to reduce their supply chain risk and give preferred vendor status to those subcontractors that respond with specific CMMC target levels, certification dates, and action plans.

Remember, CMMC cannot be applied retroactively to an RFP. As a result, the CMMC requirement will impact different defense suppliers at different times, depending on when their contracts expire, renew, or are re-negotiated.

Identifying these dates is part of Step 1 in our CMMC Best Practices Guide. If you are a defense subcontractor, it may be helpful for you to include this information as the justification of your CMMC timeline when responding to the prime contractor surveys.

Keep in mind that achieving CMMC certification earlier could present a competitive advantage for defense subcontractors. Especially this year, when we are seeing many manufacturers pivot production to different items and looking for new business opportunities, CMMC could be a key differentiator, in the same way adhering to manufacturing quality standards also positively differentiates one company from another.