Set-Aside ALERT

Business intelligence for small business federal contractors

Vol. 26, No. 21 **setasidealert.com** **October 19, 2018**

Column: Gaining a Competitive Advantage through Cybersecurity Readiness

By Jon Williams, partner, PilieroMazza PLLC

Cybersecurity is an inescapable—and growing—facet of life for government contractors. On the most recent anniversary of the 9/11 tragedy, a Homeland Security Dept. official noted that cyber threats have now replaced physical threats as the primary focus for the department protecting our Nation.

Likewise, the Defense Dept. (DOD) has been very active in promoting and regulating cybersecurity and expects that the private sector will bear the cost and responsibility for holding up their end of the security bargain.

Congress is also leading the charge, as reflected in the multiple cybersecurity-focused provisions in the 2019 National Defense Authorization Act, including a strong policy statement expressing that the U.S. should use all of its powers, including offensive cyber capabilities, to deter and respond to cyber attacks.

Contractors not cyber-ready

Yet, despite this recent attention, many contractors still have not prioritized cybersecurity-readiness.

This may be for a variety of understandable reasons, from a lack of resources to questions about whether the requirements apply to them and the likelihood of government enforcement.

When viewed only as a compliance issue, it may be easy for some to deprioritize cyber-readiness. Ignoring cybersecurity is shortsighted, though, both because of the compliance risk and also because it would be a missed opportunity to gain a significant competitive advantage in federal procurements.

Solicitations with cyber measures

Indeed, we are seeing an increasing number of federal solicitations for contracts that require demonstration of adequate cybersecurity measures.

This is happening even outside DoD procurements. For example, a recent civilian agency procurement required compliance with cybersecurity requirements very similar to what is found in DoD procurements. Offerors had to submit their information security plan as part of their proposal, and the sufficiency of the offeror's plan was a separate factor evaluated as part of the best value selection process. Soon this will be the norm, as the Federal Acquisition Regulation is expected to catch up to (and mirror) the numerous cybersecurity requirements that are already in the Defense Federal Acquisition Regulation Supplement.

As more procurements include cybersecurity requirements and evaluation factors, cybersecurity-readiness will become an increasingly important discriminator in award decisions.

In fact, DOD recently announced its "Deliver Uncompromised" initiative that is designed to make information security the "fourth pillar" of DOD acquisition decision-making, along with cost, schedule, and performance.

Additionally, most large prime contractors have mature understandings of the government's cybersecurity requirements and are actively flowing these requirements (and the resulting liability) down to their subcontractors. These realities mean that devoting time and resources to your cybersecurity is not only a compliance function, but it is a critical business development function as well.

Addressing cybersecurity

The good news is that addressing cybersecurity does not have to be a very costly undertaking. The requirements are largely malleable so solutions can be tailored to your organization and needs. For example, a very small contractor with no sensitive information in its IT system would not need to implement the same security measures as a large company with multiple IT systems handling very sensitive data.

That said, all firms, no matter the size, should have a security plan in place. And having a plan is the key first step.

Cybersecurity planning

Start by determining the cybersecurity requirements that apply to you based on your contracts and the nature of your work. This can be challenging, as in some cases you may have cybersecurity requirements in your contract that nevertheless do not actually apply to you based on the nature of your work and the information handled in your IT system.

You should work with your legal and IT advisors to determine the requirements that apply to you and the appropriate measures to implement, and then document your approach in your internal IT security plan.

NIST SP 800-171

A good place to start in developing your security plan is the "NIST SP 800-171" document. It was developed by the National Institute of Standards and Technology (NIST) to provide recommended security controls for protecting controlled unclassified information in nonfederal systems and organizations.

Compliance with NIST SP 800-171 is currently mandated for certain DoD contractors, and we have seen some civilian agencies require it as well. Compliance with NIST SP 800-171 is expected to be added to the FAR in the near future, so it makes sense to develop (or update) your plan with an eye toward the recommended security measures in the NIST SP 800-171.

IT System assessment

For most firms, developing their security plan will also involve an assessment of their current system and vulnerabilities. The 2019 national defense bill included a provision whereby DOD will help small manufacturers conduct "voluntary self-assessments," which will hopefully be expanded to more firms in the future.

For now, a vulnerability assessment could be performed in-house by your IT department or you may want to hire an external consultant to perform this for you.

It is critical to train your personnel to ensure they understand your organization's IT security measures and the importance your company places on compliance. It is a cliché because it is true: your security is only as strong as your weakest link.

Column: Competitive Advantage with Cyber

continued from page 4

Review your contracts

Another important step is to review your contracts, such as teaming and subcontract agreements, to determine if they adequately flow down cybersecurity requirements and associated liability to your down-stream partners.

And, when the shoe is on the other foot, do your contracts appropriately resist attempts by an over-zealous prime contractor to flow down cybersecurity requirements that do not or should not apply to you?

DOD cyber requirements

If your company is subject to DoD cybersecurity requirements, make sure you are registered in DIBNet (*https://dibnet.dod.mil)*.

DIBNet is where you must report a cyber incident, and you are expected to do so "rapidly." If you have a need to report, you do not want to use up precious time waiting to complete the DIBNet registration process.

Contracting officer input

Lastly, in some cases, it might make sense to talk with your contracting officers about your approach to cybersecurity requirements in your contracts.

Depending on the circumstances, the contracting officer might agree to a variance or otherwise approve of your approach that will give you comfort and certainty on compliance moving forward.

These steps may not be all that is needed for your organization, but they are a good start and a wise investment. In this environment, focusing on your cyber-readiness will pay off by reducing your compliance risk and by enhancing your competitive position with federal agencies and prime contractors.

Jon Williams is a partner with PilieroMazza PLLC law firm.