including concerns about the implementation time line and the lack of clarity on how it will be applied across different programs and suppliers. "This would have severe unintended consequences on small businesses that do not have the resources and sophistication to obtain a high CMMC level, producing market entry barriers and limiting competition," the Professional Services Council wrote in a Sept. 25, 2019 letter to the DoD after a draft release of the plan.[3]

Next Steps

If you are unsure if you need to achieve CMMC, check with your prime contractor or subcontractor. They are already preparing for accreditation and they may know if you need to attain CMMC, and at which level, to keep their business.

If you do need to achieve compliance, a good place to seek information is the National Institute of Standards and Technology Manufacturing Extension Partnership (NIST MEP) program in your state. There are MEP Centers in all 50 states and Puerto Rico. (Visit www.nist.gov/mep/mep-national-network to find the program in your state.) Your MEP center may have already launched CMMC compliance assistance seminars. If you have IT staff, it is possible to achieve the appropriate CMMC level in-house, following the NIST Handbook 162 (see Resources below).

There are also numerous CMMC Consultants online that can help companies through the process, from assessment to audit.

In Conclusion: It's Only the Beginning

When I wrote this article in the fall of 2019, the launch of CMMC seemed very fluid to me. And I recognize that I lightly touched on critical components of CMMC, in particular NIST 800-171 and DFARS. To this end, I provided a few resources below to help you learn more about CMMC. ●

[3] "Should Contractors be Fined for Their Subprimes' Cybersecurity?" by Andrew Eversden at www.federaltimes.com.

Resources

NIST Handbook 162 "NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements." Download at www.nist.gov/publications/nist-mep-cybersecurity-self-assessment-handbook-assessing-nist-sp-800-171-security.

The National Institute of Standards and Technology Manufacturing Extension Partnership at www.nist.gov/mep/mep-national-network.

Frequently Asked Questions on many aspects of CMMC are at the Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification. (www.acq.osd.mil/cmmc/faq.html)

BEST PRACTICES

Kathy Levy | Associate Editor | The Shot Peener

Seven Reasons You Need Strong Cybersecurity

1. Ransomware

According to Cybersecurity Ventures, Ransomware will have cost businesses and organizations around the world $11.5 billion in 2019 in ransom money, downtime and lost data.

2. Email

Email accounts are hacked because they are often a weak link in an organization's security pipeline.

3. Data breaches

A data breach can be caused by:

- Human error
- System glitches
- Malicious or criminal attacks

4. Laptops

Lost or stolen company laptops are a common cause for security incidents.

5. Employee theft

IBM's 2016 Cyber Security Intelligence Index found that 60 percent of all breaches are carried out by insiders, including current and former employees who—intentionally or unintentionally—take classified or proprietary information with them when they depart.

6. Lack of employee training

Do your employees know what to do when a data breach occurs?

7. Your customers

Your customers entrust you with their financial and business information. It's your responsibility to protect it. A strong cybersecurity policy should be part of your marketing materials—it demonstrates your commitment to good business practices. ●