Cybersecurity Maturity Model Certification (CMMC) Level 1

New Hampshire
PROCUREMENT TECHNICAL ASSISTANCE CENTER

It's Ready for Prime Time….

What's Driving This?

- It's all about "Basic Cyber Hygiene"
- In every industry, we are hemorrhaging sensitive information to our adversary nations, non-state actors and criminal enterprises.
- Healthcare and Financial Services have done a lot to secure their (and our) information.
- It's still "the wild west" in government contracting.
- Change is long overdue

The Rules That Frame the Requirement

- 2013 NDAA led to development of **DFARS 252.204-7012** Safeguarding Covered Defense Information and Cyber Incident Reporting. It is a rule. It applies only to defense contracts
- DFARS 252.204-7012 sparked the creation of **NIST 800-171** – the core "standard" that tells us what we have to do to comply with the rule.
- Compliance was required by 12/31/2017. There was no enforcement or meaningful support. Consequently, compliance has been insufficient.
- DoD changed its approach from voluntary compliance to mandatory certification, leading to the development of **CMMC**.
  - Based on NIST 800-171, CMMC is a multi-level, formal certification administered by 3rd parties (not the government). It is modeled after the ISO certifications.
  - Subsequent DFARS rules require concrete steps to be taken **now.** Certification will be required by 2025, **but in some cases is required today.**

But Wait - There's More!

- FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems – This contract clause probably slipped into your federal contracts and subcontracts – almost all of them, not just DoD.
- It requires you to certify that you have certain cybersecurity measures in place.
- FAR 52.204-21 is virtually identical to CMMC Level 1.
- As a result, CMMC Level 1 is becoming the basic cybersecurity benchmark for essentially all businesses.

Who Must Comply?

- Applies to contractors & subcontractors at all tiers
- There are exemptions for:
  - Micropurchases – Purchase Card buys under $10,000
  - COTS contracts – contracts for commercial, off-the-shelf items
- However, that doesn't matter. **It's time to get your cybersecurity act together.**
  - **This is not going away.**
  - **The dust has settled – the basic standards are clear**
  - **Because it's technology-driven, change is constant – but it will be incremental.**

How Much Will It Cost?

1. **How badly do you want to be in business?**
2. Costs will vary greatly, depending on the size and complexity of your business, and the degree of your reliance on IT.
3. There are four categories of cost to understand:
   - Initial cost to get into compliance
   - Costs to get certified (if required)
   - Ongoing costs to maintain secure systems
   - Future Update/upgrade costs driven by
     - Business growth/change
     - Technology changes
4. **Costs will be significant.**

Let's get to the Nitty-Gritty

- 17

Self Assessment and Score Reporting

- You should perform an honest self-assessment. Self-Assessment guidance and tools are readily available.
- If you are a defense contractor, subcontractor or supplier, you may have DFARS 252.204-7019 in your contract. If so, you must upload your score into a DoD database called the Supplier Performance Risk System (SPRS).
- SPRS is accessed through the Procurement Integrated Enterprise Environment (PIEE). If you sell to DoD, you are probably already familiar with PIEE as the home of Wide Area Workflow (WAWF), DoD's online invoicing tool
- NH PTAC can help you understand what you need to do and how to submit your score through these systems

Conclusions

- Almost everybody needs to get to Level 1.
- Currently, you only will need to be certified if you are a DoD contractor or subcontractor. Expect this to expand in time.
- It will take some time, and will probably cost money.
- Procrastinate or ignore this at your peril
- Management buy-in is critical
- Your IT staff will be responsible for many of the details, but they should not lead your program. Management must take the lead.

Key Resources

- NIST 800-171
  - Includes further links to POAM Template, SSP Template
- NIST SP 800-171 DoD Assessment Methodology, Version 1.2
- CMMC
- CMMC Accreditation Body
- CMMC Model and Assessment Guides
- Cybersecurity and Data Protection, North Star CMM (an ASBDC tool)

More Resources

Cybersecurity Referrals:

Mainstay Technologies
www.mstech.com
Ryan Barton, CEO
201 Daniel Webster Highway
Belmont, NH 03220
(603) 524-4774
info@mstech.com

Monarch Information Security Consulting
https://monarchisc.com/
Joe Kurlanski
Saco, ME 04072
(207) 808-0472
info@monarchisc.com

Patriot Cyber Defense
www.PatriotCyberDefense.com
Jennifer Caron, President
(603) 231-7000
Jennifer.Caron@PatriotCyberDefense.com

Project Spectrum
https://www.projectspectrum.io

RegDox Solutions
www.RegDox.com
William O'Brien, President/CEO
1 Tara Blvd #300
Nashua, NH 03062
(603) 589-4830
wobrien@regdox.com

Summit Cyber Solutions, LLC
www.summit-cyber.com
David Kuhns, CEO
One Stiles Rd Suite 105
Salem, NH 03079
(202) 559-8988
David.Kuhns@summit-cyber.com

Wapack Labs LLC
https://www.wapacklabs.com/
Jeff Stutzman
326 Chestnut Hill Road
New Boston, NH 03070
(603) 930-2222
sales@wapacklabs.com

Please note: NH PTAC does not endorse professional service providers, and makes no representation as to the fitness of any of the above firms to provide services in regard to your needs.

Thank you!

New Hampshire Procurement Technical Assistance Center
Division of Economic Development
Department of Business and Economic Affairs
100 North Main Street, Suite 100
Concord, NH 03301
603-568-8485
nheconomy.com/sell-to-the-government
Email: govcontracting@livefree.nh.gov

Deborah Avery Danielle Bishop Jane Brezosky Larry Findeiss Dave Pease