DoD Cyber Incident Compliance – Compliance Deadline 12/31/2017

For defense contractors and subcontractors, the **cybersecurity** requirements of DFARS 204.73 and the clauses at 252.204.7008, 7009, and 7012 have been an issue since they were enacted in 2013 and rolled out Dec. 30, 2015. When originally enacted the rule referred to a vague NIST standard, which did little to explain what compliance would look like or how it could be accomplished. In October 2016 a final version of the NIST Standard 800-171 resolved and clarified compliance.

NH GovCon can direct you to services offered by NH MEP, private IT consultants and commercial software products to help small businesses that are subject to this rule. ***At the present time, DoD deems that having a formal, documented plan for compliance is sufficient and is deemed compliant.***

"Contractors must document the state of their information system in a 'system security plan' and document how and when they will implement any 'not yet implemented' requirements in associated plans of action."

Here is a very basic checklist to explain what is needed; you'll need to have a plan, including a schedule, to implement anything that is not yet in place.

Small Business Cyber Awareness Checklist

1. Protect against viruses, spyware, and other malicious code—Install updates regularly
2. Secure your networks—Use firewalls. Encrypt data. Password protects areas.
3. Establish security practices and policies to protect sensitive information—Establish and enforce policies.
4. Educate employees about cyber threats and hold them accountable—Set standards. Train regularly. Inspect what you expect.
5. Require employees to use strong passwords and to change them often—Institute multifactor authentication processes.
6. Employ best practices on payment cards—Work with your banks or card processors to ensure the most trusted and validated tools and anti-fraud services are being used.
7. Make backup copies of important business data and information—Back up regularly—and remotely.
8. Control physical access to computers and network components—Prevent unauthorized access.
9. Create a mobile device action plan—Establish BYOD policies. Password protect, encrypt data, and install security app. Report lost or stolen equipment immediately.
10. Protect all pages on your public-facing websites, not just the checkout and sign-up pages—Protect all of your site data. Install a web application firewall. Hide the admin pages. Limit file uploads. Use SSL

1. Here is a link to the June Cybersecurity conference that we organized that you might find helpful. http://www.nheconomy.com/getmedia/a93dcf47-c21e-4432-8da0-053a3a9cbdd8/3-NIST-Presentation-Patricia-Toth.pdf
2. Here is a link to the most current version of the NIST Standard: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf
3. NIST SP 800-171 makes reference to another NIST Special Publication – NIST SP 800-53. You can find this at: https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf
4. NIST has gone another step by producing a "Self-Assessment Handbook" which is available at: https://www.nist.gov/publications/nist-mep-cybersecurity-self-assessment-handbook-assessing-nist-sp-800-171-security
5. DPAP maintains a cybersecurity page at www.dodprocurementtoolbox.com to include guidance on how a small business with limited information technology or cybersecurity expertise might approach meeting the cybersecurity requirements, guidance addressing the December 31, 2017 deadline for implementing NIST SP 800-171, frequently asked questions addressing concerns identified through our communications with industry, and videos, webinars, and briefings addressing the requirements of DFARS Clause 252.205-7012 and NIST SP 800-171.

An excellent source of assessment & training is the NH Manufacturing Extension Partnership: http://www.nhmep.org/.