BDO KNOWS:

GOVERNMENT CONTRACTING

CYBERSECURITY FOR GOVERNMENT CONTRACTORS: NEXT STEPS

The U.S Department of Defense (DOD) has implemented new cybersecurity requirements for defense contractors via the DOD Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, which became effective December 31, 2017. This DFARs clause requires all defense contractors to implement information security programs to protect their Controlled Unclassified Information (CUI) in Non-Federal Systems and organizations in accordance with the National Institute of Standards & Technology (NIST) Special Procedure (SP) 800-171.

NIST SP 800-171 provides 109 individual security controls which are categorized under 14 families of information security requirements. It is widely expected that this set of cybersecurity requirements will be extended beyond defense contractors to all government contractors via a new final rule to the Federal Acquisition Regulation (FAR) during 2018.

It is not surprising that many government contractors, especially defense contractors feel overwhelmed, as they must now comply with several new requirements on top of the numerous industry-specific and international cybersecurity standards, such as ISO 27001. So, now that defense contractor's information security system must be compliant with NIST SP 800-171, government contractors are asking "What is Next…"

CONTACT

GREGORY GARRETT
Head of U.S. & International Cybersecurity
703-770-1019
ggarrett@bdo.com

CYBERSECURITY FOR GOVERNMENT CONTRACTORS - WHAT IS NEXT...

1. Expect the Defense Contract Management Agency (DCMA) to begin conducting information security reviews/assessments of major defense contractors and selected mid-sized defense contractors in early 2018.

It is expected that DCMA may request a copy of the contractor's System Security Plan (SSP), Incident Response (IR) plan, and a copy of their information security policies and procedures for each of the 14 information security categories contained within NIST SP 800-171.

2. Anticipate the Defense Contract Audit Agency (DCAA) to develop audit guidelines related to information security management systems' cost accounting and begin conducting audits for cost allowability and reasonableness by mid – 2018.

It is expected that the New DFARS 252.204-7012 cybersecurity and information security management system will be treated in the same manner as the current six major DFARS contractor business systems: accounting, cost estimating, Material Management and Accounting System (MMAS), government property management, and Earned Value Management System (EVMS).

3. Expect a few large and mid-sized defense contractors to be determined to be non-compliant with all or part of the DFARS 252.204-7012 and NIST SP 800-171 requirements by mid-to-late 2018.

It is expected that some contractors will be given a variety of remediation actions and/or penalties as deemed appropriate by the respective Government Contracting Officer, which may include:

- Withhold of contractor payments.
- Issue a Stop Work Order.
- Issue a Suspension of Work.
- Terminate the contract-for default.
- Place the contractor on the government ineligible contractor list.

4. Anticipate the issuance of a new FAR Final Rule Creating Cybersecurity requirements for all U.S. government contractors by late 2018.

It is expected that the Federal Acquisition Regulatory (FAR) Council will enact a new FAR Cybersecurity Final Rule for all government contractors, which will be quite similar in nature and content as the current DFARS clause.

5. Expect a new wave of government contractors conducting internal cyber risk assessments and compliance gap analysis per NIST 800-171 information security requirements by late 2018 and early 2019.

It is expected that a new wave of government contractors will conduct internal risk assessments, after the DCMA information security system reviews and DCAA audits on defense contractors are conducted containing numerous negative audit findings. Plus, the issuance of a new FAR Final Rule for cybersecurity requirements for all government contractors will further increase the demand for independent cybersecurity risk assessments and compliance gap analysis. Many government contractors will become highly focused on improving their respective information security policies, processes, and procedures, with increased focus on – monitoring, detection, incident response, business continuity planning, disaster recovery, and third-party information security management.

6. Anticipate a New Public Law (PL) for Cybersecurity to be established for consistency in Cyber Incident Response Reporting and Timely Remediation Actions for Cyber Breaches for all Publically Traded Companies in 2019.

Based upon the increasing number of cyber-attacks and the growing financial impact of recent cyber breaches, especially upon large publicly traded companies, it widely expected that the U.S. Congress will enact a New Public Law to establish some consistency in cyber incident reporting with specific requirements for timely remediation actions post-breach with appropriate penalties for non-compliance.

7. Expect the global shortage of experienced cybersecurity professionals to increase over the next three to five years.

Thus, the need to create the right balance of cybersecurity employees, automated tools, and outsourced or managed security services will became vital to all public and private organizations, especially for small to mid-sized companies.

SUMMARY

As government contractors are required to comply with New U.S. regulatory requirements, they are experiencing a rise in compliance related costs. It is well known that many government contractors will sometimes decide to defer these additional compliance related costs to see if the government will enforce the new information security requirements. If the cybersecurity requirements are enforced by the government, as we expect they will be, the government contractors will often wait to see how much the penalties are and if the cost of the penalties are greater than the cost of compliance to decide whether they should bear the additional expenses.

Government contractors now find themselves facing a growing business dilemma: They must figure out the best way they can properly safeguard their CUI, ensure regulatory compliance while continuing to remain competitive in the Federal Marketplace, and achieve a fair and reasonable return on investment. Meanwhile, we fully expect the U.S. Federal government to continually evolve and expand their cybersecurity regulatory requirements for government contractors.