DoD Contractors: Take Control of Your Cybersecurity Before an Audit

Compliance Audits are Coming based on DFARS 252.204-7012 and NIST 800-171 Guidelines

The deadline for federally mandated cybersecurity has come and gone, yet compliance still looms over many DoD contractors. While contractors know that it's the cost of doing business, the complexity of enhanced protection, cost of maintaining and managing security, and simply not having the right expertise make compliance a challenge. The truth is that documentation and policy aren't enough though.

As standards become more stringent and security threats continue to evolve, contractors need to maintain state of the art security. While requirements laid out in DFARS 252.204-7012 and guidelines in NIST SP 800-171 provide a roadmap to "adequate" security, contractors need to find a cost-effective option that provides advanced, managed security protection from cyber threats

Winning bids means DFARS compliance.

Since 2010, the Department of Defense has increasingly focused on protecting controlled unclassified information (CUI) held by contractors and their subcontractors. Ad hoc policies and procedures weren't seen as enough to safeguard information from cybercrime and espionage. DFARS and NIST SP 800-171 provides a set of security controls for contractor information systems that hold CUI. Now, any company that generates revenue selling to DoD-related businesses needs to be compliant. Basic security, however, may not be enough. Cyber threats are only becoming more advanced and if information is compromised it means lost contracts.

Three roadblocks: complexity, cost, and expertise.

Compliance with cybersecurity requirements isn't just complex, it can take an exorbitant amount of time and money. Beginning with an assessment of over 110 controls, contractors need to develop a system security plan (SSP) describing how all of the requirements are met, as well as a plan of action on how any pending requirements will be met. Requirements range from one-time implementations such as multi-factor identification and authentication, to ongoing processes such as monitoring and incident response protocols. Many, if not most, contractors don't have the internal resources to manage these requirements. For those that do try to handle compliance internally, a DIY approach can not only be expensive, it can totally miss the mark.

Is meeting requirements enough?

Cyber security requirements from the DoD have been around for years. For contractors supporting the DoD, network security is a prerequisite to winning bids. In fact, over 87% of contracts with the Department of Defense (DoD) in 2017 had federally mandated cybersecurity requirements. However, while it seems like compliance is enough, it is only meant to provide "adequate" security. It may not actually be enough to protect systems from ever-changing cyber threats. What happens if security is breached, because adequate security wasn't enough? What happens when competitors have more advanced network security in place?

Additionally, not only is security becoming a performance and reward differentiator, but DoD-sponsored 3rd party audits are beginning. This means, there's no time left to ease into compliance; contractors can lose their business if they aren't in compliance. Additionally, security threats are far from static. Once compliant doesn't mean always compliant. Standards are only becoming more rigorous as threats evolve and become more sophisticated. Which means contractors always need access to the most current cyber security technology.

Security, simplified.

ZenOpz provides a simple, cost-effective way to take control of DFARS compliance. Our network monitoring scans 24/7 for vulnerabilities and allows contractors to effectively close up any loopholes in their security policy. Our technology evolves with the most current threats as well as any changes to the regulatory environment. When threats do crop up, we have security experts on standby so that incidents can be dealt with swiftly. Taking the complexity and cost inefficiencies out of the equation means that contractors can check DFARS compliance off their list focus on winning bids.

Call us at **571-282-4426** or email **info@zenethtechpartners.com**
to find out how you can have a simple, cost-effective way to be DFARS compliant.