Webinar: How Changes in DFARS Cybersecurity Enforcement Can Impact Your DoD Business

written by Lauri Moon | August 17, 2018

DoD contractors have been required by the 7012 DFARS contract clause to have "adequate security" in place by 1/1/18 relying upon the 110 NIST SP 800-171 safeguards. Initially, DoD advised that companies could consider themselves to be in compliance if they prepared a System Security Plan (SSP) and Plan of Action and Milestones (POAM). These remain core requirements — but minimal compliance will not be enough. DoD is moving towards a more aggressive approach to assure that its contractors in fact have implemented adequate security measures.

Soon, DoD requiring activities, contracting officers and oversight personnel will be asking to review defense contractor SSPs and POAMS as part of the procurement process. We can expect DoD to establish means to assess contractor security – almost certainly relying upon the new NIST SP 800-171A "Assessing Security" guide. Companies may find themselves ineligible for new procurements if their security is found inadequate. New solicitations will include assessed cyber security as an evaluation factor and therefore a discriminator in future contract awards. What this means is that changing DoD practices will have significant impact on a company's ability to win and perform work on Government contracts. There will be increased attention to security at all levels of the supply chain and we can expect the Government to hold Primes responsible to assure the compliance of their suppliers. These changes reflect an emerging recognition within the Pentagon, that adversaries continue to successfully exploit cyber vulnerabilities of the U.S. industrial base, and a new determination to take stronger measures to protect critical technologies. DoD leadership will seek to reward companies with superior security as well as enforce existing cybersecurity regulations.

In this webinar from the Cyber Collaboration Center, DFARS / NIST cybersecurity experts from eResilience are teaming up with leading industry analyst, author, and legal counsel Robert Metzger to provide updates on new DoD-wide initiatives,

changing defense procurement policies, and what lies ahead for contractors in Government oversight and assessment. Topics to be covered include DoD's newly announced "Deliver Uncompromised" initiative, how DoD is to value and assign priority rankings to the 110 NIST 800-171 security requirements; where to expect new cyber measures in solicitations and competitive selection; supply chain cyber risk management challenges; and the establishment of Security as a "Fourth Pillar" in defense acquisition equal in priority to Cost, Schedule and Performance. In this webinar, eResilience subject matter experts will discuss challenges facing defense contractors including the importance of supply-chain cyber risk management (SCRM), and Bob Metzger will share his insight on cyber and supply chain security trends. Don't miss this opportunity to learn from some of the industry's top technical and legal experts.

Speaker: Robert Metzger

Bob Metzger is one of the top rated defense contract law experts in the country. Named a 2016 " Federal 100 " awardee, Federal Computer Week cited Bob for his "ability to integrate policy, regulation and technology." Chambers USA (2018) ranks Bob among top government contracts lawyers and said that "[h]e is particularly noted for his expertise in cyber and supply chain security with clients regarding him as the 'preeminent expert in cybersecurity regulations and how they affect government contractors.'" He was a member of the task force that produced the 2017 Defense Science Board Cyber Supply Chain Study. Bob is a frequent contributor to defense industry publications, and a consistent advocate for improvement of the nation's cyber defenses.

Who Should Attend:

Defense Contractors & their Executives, Contract Managers, Program Managers, IT Managers & FSOs

Register