Cybersecurity Trends for 2019 and Their Impact on DoD Contracting

written by Lauri Moon | January 7, 2019

This webinar will focus on the Government's tightening and increasing cybersecurity requirements for defense contractors that can greatly impact future business. It is important for companies to stay on top of these changes and apply strategies to minimize impacts. Learn about these trends and what proactive companies are doing to identify and reduce risks. Major supply chain vulnerabilities are the desired attack vector of foreign adversaries, especially targeting smaller and less protected businesses. The U.S. Government is making policies to combat these threats. As cybersecurity guidance and requirements for government contractors continue to evolve and grow, it is important to understand how flow-down clauses may affect subcontractors in the supply chain – and how the cybersecurity risk of the supply chain can impact federal procurement decisions.

This webinar will cover:

- Cyber attacks: The evolving threat landscape
- Government cybersecurity policy trends for 2019
- Creating security policies relevant to today's cyber threats
- Why "point-in-time" attestations are not sufficient
- How to manage regulatory challenges by focusing on "Continuous Compliance"
- The movement toward validating subcontractor compliance self-attestations
- New requirements prime contractors are demanding from suppliers and subcontractors

Speakers:

Tim Williams, Technical Director, eResilience

Mr. Williams is a Chief Security Architect with expertise in DoD/NSA cross-domain security architectures and enterprise systems. He has over 34 years of success in providing product design, development, and integration guidance for commercial and government secure and accredited systems. Mr. Williams is a subject matter expert for design and deployment of NSA Commercial Solutions for Classified (CSfC)

systems and support for customers implementing NIST RMF, DoDRMF and NIST Cybersecurity Frameworks. He has performed risk and security control assessments based on NIST guidelines (800-30 and 800-53a) for public and private organizations and has worked with DoD red and blue teams during large cyber exercises. Mr. Williams has developed and worked through the evaluation process for meeting the FIPS 140-2, Common Criteria EAL-4 requirements. He holds six patents in the multi-level security area and secure virtualization.

Dianna Ho, Vice President of Marketing, eResilience

Ms. Ho is the Vice President of Marketing for eResilience. She focuses on alignment between eResilience's technology innovations and delivering customer centric solutions to help government contractors meet and manage their cybersecurity requirements and supply chain compliance flow-down. With 20 years of experience in the technology and cybersecurity space, Ms. Ho is a strong advocate for purpose-built approaches to cybersecurity, driven by a thorough understanding of the needs of the customer, the evolving cyber threat landscape and upcoming regulatory actions. Ms. Ho has successfully brought solutions to market for top, leading-edge small and large global technology organizations across the channel, including Ingram Micro, M86 Security (acquired by Trustwave), Belkin Government and Linksys.

Register