"Help Me, Help You": Defense Department Advises Contractors That Cybersecurity Is An Allowable Cost [VIDEO]

Monday, June 24, 2019

During a presentation at the Professional Services Council Federal Acquisition Conference on June 13, 2019, a high-ranking Department of Defense ("DoD") official announced, with dramatic flair, that cybersecurity is an allowable cost:

*"I need you all now to get out your pens and you better write this down and tell your teams: Hear it from Katie Arrington [Special Assistant to the Assistant Secretary of Defense for Cyber] . . . **security is an allowable cost**. Amen, right?"*

Channeling *Jerry McGuire*, Arrington added: "Now what you need to do as industry is help me, help you. I'm not the enemy. I'm literally the one person in government who said, 'Hi, I'm here to help and I'm legit here to help.'"

jackson lewis.

Article By   Damon W. Silver
Catherine R. TucciarelloJackson Lewis P.C.
Workplace Privacy Blog

Government Contracts, Maritime & Military Law
Communications, Media & Internet
All Federal

Arrington's June 13 presentation, which was titled "Securing the Supply Chain," is just the latest indication that the DoD – like other federal and state agencies – is making the cyber hygiene of its contractors a priority. (Some of our previous posts on this topic are available here.)

During a webinar earlier this month, Arrington noted that, "[i]f we were doing all the necessary security controls, we wouldn't be getting exfiltrated to the level that we are. We need to level set because a good portion of our defense industrial base [("DIB")] doesn't have robust cyber hygiene. Only 1% of DIB companies have implemented all 110 controls from the National Institute of Standards and Technology. We need to get to scale where the vast majority of DIB partners can defend themselves from nation state attacks."

Arrington, who appears to be actively involved in the DoD's development of a cybersecurity assessment and certification program, called the Cybersecurity Maturity Model Certification or CMMC, provided additional details about that program during her June 13 presentation.   Specifically, Arrington announced that:

1. The CMMC will include five levels of certification. The levels will range from "basic" cyber hygiene to "state-of-the-art."

2. The CMMC initiative will require DoD contractor information systems to be certified compliant by an outside auditor. Under the new model, third-party cybersecurity certifiers will "conduct audits, collect metrics, and inform risk mitigation for the entire supply chain," Arrington said. "Every contract that goes out," she added, "will have a requirement and every vendor on that contract will have to get certified."

3. The DoD will hold 12 listening sessions across the country this summer to solicit feedback about the CMMC from industry and other experts.

4. The DoD aims to complete the CMMC and begin certifying vendors by January 2020; to begin incorporating the CMMC requirements into requests for information by June 2020; and to include the CMMC in solicitations by September 2020.

Driving home her key point that the cybersecurity of its vendors is a major priority for the DoD, Arrington stated that "[c]ost, schedule and performance are only effective in a security environment." She added that "[w]e cannot look at security and be willing to trade off to get lower cost, better performing product or to get something faster. If we do that, nothing works and it will cost me more in the long run."

DoD contractors should heed Arrington's warning that cost, schedule, and performance will not alone suffice to win future DoD contracts. To best position themselves to compete for those contracts, contractors should consider providing feedback to the DoD this summer about the CMMC, and should promptly begin the process of preparing to comply with its mandates.

Jackson Lewis P.C. © 2019

Source URL: https://www.natlawreview.com/article/help-me-help-you-defense-department-advises-contractors-cybersecurity-allowable-cost