Meeting Notes: NeoSystems Town Hall Meeting, 24 March 2021

Attendees:

Mr. Ed Bassett, CISO, NeoSystems Corporation

Stuart Itkin, Vice President, CMMC and FedRAMP Assurance for Coalfire Federal, based in the Washington DC Metro Area

Stuart Itkin is vice president of CMMC and FedRAMP assurance at Coalfire Federal. His background is in marketing and product development specifically in the cybersecurity space. He previously worked at Exostar at SIFE. He's also a mentor with the MACH37 cyber accelerator. Coalfire Federal is already the largest player in the FedRAMP 3PAO space, having done more assessments than anybody and Stuart looks to lead them down the C3PAO path as they move to support CMMC.

The discussion was centered on CMMC certification and the challenges faced by the known 300,000 persons within the defense industrial base who must achieve certification.

Itkin discussed competitive advantage. He says that contractors understand the value of individuals and other contractors they bring onto a bid and being CMMC certified. This makes firms and individuals more attractive to those they want to do business with.

He also points out that cost is a confusing topic when it comes to CMMC as certification is probably the smallest cost component. It's really the cost of getting ready, understanding where they are today relative to being able to achieve the required level of cyber maturity and the things that they need to put in place to be able to get there, those influence cost more.

Itkin says we can expect to see automated tools to move assessments along, check configurations, and check compliance with specific requirements that may exist. Itkin also believes various innovations are being brought to market to help organizations achieve the requisite level of cyber maturity from organizations that are specifically developing solutions.

There was much discussion about prioritizing who should first be allowed to attain certification.

Stuart Itkin replied that his firm has queried the accreditation body asking for guidance relative to those organizations involved in the pilot programs and the order of priority for certification. Itkin stated: “We've not received any specific guidance that point others than being told, 'It's a good question."

Itkin said at present the backlog is building and continuing as organizations come to his firm. "But we expect that we will get some guidance from the accreditation body with respect to those organizations that are part of the pilot program."

Ed Bassett asked of Itkin, from a C3PAO perspective, what can we all expect from assessments? How are they going to be carried out? What kind of level of knowledge, experience training, et cetera, should we expect from the assessors? And then sort of on the ground experience, how do you see that coming to be?

Itkin replied that the perspective is that this is a hundred percent conformance standard that needs to be met. It's not one like others, like FedRAMP or 800-171. Organizations coming into the assessment process need to have a high degree of assurance that they've truly satisfied all of those practice requirements and the role of the assessor; again it's not to provide feedback, he explained, but rather simply to be able to provide, pass/fail information back to the organization that is seeking certification.

Itkin recommends they go through a readiness assessment. This is something that can be conducted by a C3PAO, is not a conflict and can be conducted by another organization.

As the meeting wound down, and questions from the audience continued, someone asked: "You talk about showing an auditor that we satisfy a control, but then you mentioned maturity. What are the requirements and expectations for showing maturity? Do we have to prove that our policies and procedures have been satisfied and improved over time?"

Itkin that the answer to the latter is yes and that there is some discretion in substantiating that to sufficient satisfaction. Said Itkin: "A lot of people ask specifically, 'well, how much evidence do I need to provide? Do I need six months? Do I need three months?' And the guidance has been left to the discretion of the assessor to be able to establish in their judgment that the organization has achieved maturity, that they have developed and implemented the control. They're following it, they're using it and that it's proving to be effective."