**Meeting Notes - NeoSystems Town Hall Meeting - 28 April 2021**

**Attendees:**

 *Mr. Ed Bassett, CISO, NeoSystems Corporation*

*Mr. Tony Bai,* *Federal Practice Lead at A-LIGN in Tampa, Florida*

Tony Bai is the federal practice lead for the cyber risk advisory firm, A-LIGN. He's been performing cyber risk assessment and advisory services in the federal sector for the past seven years. Prior to that, he served a full career in the Air Force for over 20 years, working in cyber warfare, and cyber defense in IT operations. Tony's firm is a candidate C3PAO, and one of the very first to move through that process. His perspective on cyber audits spans all the current compliance frameworks. He is well grounded in the pragmatic experience that he has of how real systems are managed day to day.

The meeting began with Tony describing the process of being an approved C3PAO candidate. He explained that it entails submitting your application to the AB. Upon acceptance, it goes through a review process with them and the DoD’s CMMC program management office.

The approval process looks at any foreign ownership or affiliation. Upon approval, they became a candidate C3PAO. This means they are working with the DIBCAC out of DCMA to schedule MMC level three assessments to be performed on them.

Once A-LIGN attains CMMC level three certification, they may perform assessments as an organization with their own certified assessors or provisional assessors and things of that nature.

Bai says that even if you have experience in other frameworks, CMMC is still its own entity. Those who have participated in other federal framework assessments, like risk management framework for FISMA and FedRAMP are probably going to be the most comfortable with CMMC according to Bai.

"Those that are doing like SOC 2s or ISO 27001 or PCI, they're going to have adjustment," he says. "It's more about a culture adjustment, right? So, remember, this is being reviewed by, at the end of the day, government personnel. It's a very, I guess you'd say, prescriptive framework, where they outline a lot of the assessment standards that are a little bit less or a little bit vaguer in some of the other commercial frameworks. Not saying that the government frames are worse or anything like that, it's just more of it's a different mindset with the federal."

He adds that if a company has gone through FISMA or FedRAMP they already have some preparation. FISMA and FedRAMP are based on NIST Special Publication 800-53 controls, which are the basis of where the CMMC practice come from. This may make the transition easier.

Regarding the timing of CMMC, Bai believes companies will be driven by the likelihood of winning a contract before ramping up to be prepared for the CMMC framework and meeting all practices. Right now, 100% compliance is required for award of a contract. The time between RFP and award may not be enough to meet all findings from an audit prior to certification, and ultimately award.

In preparation for CMMC, Bai says it's a corporate culture change in establishing best practices of cybersecurity. "So, what I'm going to look for is a configuration change for a CCB of some sort," he says. "So now, as a C3PAO auditor or CMMC, I'm going to ask for pieces of that as demonstration. Like what are the meeting minutes when the board met? What were the items discussed? What was the review process? Where did you approve it? How do you approve it? What was the follow-through? All that should be outlined within the policies and procedures that demonstrate your maturity of implementing those controls. That is the type of thing that, for me personally, as an assessor, what I would ask for and look for."

Tony Bai also advises that firms have an external consultant to help attain certification, rather than try to conquer it with in-house assets. "Companies aren't in the business of understanding federal cybersecurity requirements, unless you're a cybersecurity company and that's where you deal with," he says. "Their jobs are to provide the specific capability or services they offer that are a value to the DoD. It is not meeting CMMC requirements or FedRAMP or FISMA. So, I've always been a big proponent of why try to build that in-house knowledge? Why not bring in that person that that is their job, that is their living, right? Now, I was always told, "If you don't do it for a living, you should hire someone that does." Right? It just saves you money, time, and effort down the line. So, I'm a big proponent of using consultants or advisors."

Bai expects some change as time goes by and ambiguity and unanswered questions rise to the surface when attaining CMMC compliance. He says the required level of certification will reside as a contracting officer's decision in many cases, pre-solicitation.

 "The DoD contracting officers are going to specify a level for each contract," he says. "As that flows down, the required level of the subcontractor may be different, lower particular than the overall contract, depending on the services that are being provided, and the kind of information that's shared with that subcontractor."

After some audience questions the town hall wrapped up. Tony Bai said "it really comes down to proper preparation, which means understanding the CMMC practices and processes and what those objectives are, right? Because the goal there is for you guys to look at those and internalize those to create a proper cyber security program over the people, processes, and technology, right? It's about protecting the data. Now, on the practical level, it's about getting your certification so you can feed on the contracts. All we are going to do is we are going to go abide by the outlined guidance. So that is up each company to really understand that, whether they want to do their own analysis or hire someone else to help them and make sure what they are doing meets those requirements. If not, then address those gaps."