**Meeting Notes: NeoSystems Town Hall Meeting, 21 April 2021**

**Attendees:**

 *Mr. Ed Bassett, CISO, NeoSystems Corporation*

*Ms. Amy Howland, Vice President, Chief Information Security Officer (CISO) at Perspecta*

Amy Howland has over 20 years of experience in cybersecurity and information assurance, including work as a CISO for CSRA, now part of General Dynamics Information Technology. She also worked at Blue Canopy, Avaya Government Solutions, and Ernst & Young. She brings practical, real-world experience and is among the best prepared in responding to the CMMC mandate.

Discussion began with Ed Bassett asking about CMMC and how it may change priorities for Perspecta and if it includes a refocus on processes that have already been in progress at Perspecta.

Howland says it's probably a mix of both. She notes that within an IT organization and with all the projects underway within it, CMMC has brought security issues to the forefront in understanding how serious this needs to be. She adds that CMMC comes with milestone deadlines that inserts more urgency into taking measures to be compliant and therefore engenders best practices when it comes to issues of CUI and cybersecurity.

Howland says her organization has come up to speed by reading and studying the requirements and collaborating with others regarding it.

"We realized early on that it, even though these are cyber controls and relating to NIST, much resides within the cyber organization," she says. "Then within IT, we realized that this was bigger than that, and I think it took a while for everyone to fully grasp it including myself, and that it's really dependent on a lot of other organizations. And there's your physical security, your human resources, your facilities; all the folks that if we're going to have mature processes in place that need to be documented. We needed to all work together. So, those were other things we started doing and setting up those meetings and discussions earlier on."

Howland added that CMMC has forced more collaboration than in the past. She compares cyber security to physical security, by saying that physical security had definite processes related to badging and entrance privileges. CMMC is putting more urgency in boosting cyber controls and ensuring you have all the right information and making sure that what you're saying is not just about one location, for example, but implementing controls across the board from a corporate perspective.

She says the timeline has pushed the attention to CMMC and is forcing measures to be promptly taken. She notes that if you look at the timeline of what's happened with CMMC from when it came out in January 2020, the timeline events from setting up the accreditation body, to getting the controls out, to get any appendices established, you can see how quickly it is moving.

"I think that folks really do need to pay attention, need to take this seriously," she says. "Maybe take it as a gift that, in fact, there it is slipping because there's a lot to do. It's not what we've all been trying to accomplish in the past. Just being compliant with our NIST 800-171 controls, do you pass or not? This is about maturity and processes and really having a great mature program in place. So, I think that the other thing is that this is a DFARS formal regulatory rule. I think that really clinches the fact that this is real, and this is happening. It's just a matter of when everything gets signed."

She also points out that strategic partners must be compliant, and they may be part of the team that you're approaching a proposal with. Now it means that your partners must have the required controls in place for you to bid and capture business via proposals. This is all new and an added responsibility by all.

"We sent out a couple of memorandums and basically made sure that folks were aware of CMMC, aware of what they needed to do," she says about Perspecta's efforts. "We had a call, we entertained questions, and we provided some avenues of where they might get some resources to help, to get them ready for the controls that they had to be compliant with."

She remarks that when you're doing that assessment, it's the IT ops teams that must demonstrate the trust and substantiate and bring forth cyber into everything that they're doing and help folks throughout the enterprise understand why you're asking to do something. She says that IT operations personnel at the firm are bringing cyber in every conversation. "I think that's really what's important to help drive the mission to get people involved," she says.

The conversation concluded with Howland emphasizing that CMMC is reason to keep momentum building in creating sharp cyber controls. It will be part of the future and intrinsic to doing business with DoD into the future. She says:

"Continuous monitoring is a standard cyber buzzword, but if you've done all this for CMMC, keep it going, keep it up and continue to look at your processes that you have documented and mature those processes. And really, it's giving you a better cyber program. It's securing your company. And then, oh, by the way, you're also compliant and able to bid and receive awards, but just look at it as a program, not a one-time thing, and it will encompass everything you're doing."