**Meeting Notes - NeoSystems Town Hall Meeting – 19 May 2021**

**Attendees:**

*Mr. Ed Bassett, CISO, NeoSystems Corporation*

*Amy Howland, CISO for Perspecta (now part of Peraton)*

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 Technologies. She also held cybersecurity leadership roles at Blue Canopy, Avaya Government Solutions, and Ernst & Young.

The DIBCAC, the Defense Industrial Base Cybersecurity Assessment Center audited Perspecta recently. She recently was a guest on a previous NeoSystems town hall and has returned to share her experience with their recent audit.

The conversation began with a discussion of assessment standards: NIST 800-171A lays out three different assessment types. The DFARS 70-19 rule calls these basic, medium, and high.

Howland's organization recently undertook the high assessment. She stated that the moderate or medium level assessment appears to be more of a review of your system security plan and how you are responding to how you're implementing controls. The high assessment is more of an interview, demonstration, review, and more in-depth look. Because Perspecta's expectation is to pursue level three CMMC assessment it would require the more in-depth review, thus the high assessment.

Perspecta moved forward with a DIBCAC assessment. To prepare they had help from a third-party assessment organization who assisted them, as wells an internal team. She explained that they had an "artifact" for each required control.

"The controls can hit so many different areas," she says. "You're answering the control, but are you answering it for workstations and servers and network devices, because in companies fortunate to have multiple teams to address those areas, it's different people, different processes, still getting to the same end state. So, we had to make sure that we had an artifact or a show-me ready for every one of those areas to address the control and the control objective."

Regarding the artifacts to satisfy the conditions specified as controls, Howland advises using the CMMC Level 3 Assessment Guide. "It's excellent," she explains. "Not only does it give you the control, but it also then gives you the detailed information, the technical information about that control, and then it provides a scenario. And the scenarios, I feel they're more suited a bit towards smaller businesses, but it still gives you a sense of the idea of what are they looking for? What is this control really talking about?"

Audience questions included an inquiry about what "systems" within the company's operations included CUI and which did not. Is there a reasonable way to separate the two?

Howland said they structured theirs as a network diagram. "We structured ours, and that was another thing that we really fine-tuned and honed as we were getting ready, is made our network diagram better," she explains. "We sort of overlaid the network diagram that we had, a high-level network diagram, that showed different Perspecta systems, data centers, some of the cloud pieces, and we showed the whole picture. And then we had a boundary that was the corporate network boundary that excluded, obviously, a lot of the SAS. I mean, we're not doing an assessment of our SAS providers, it's what we use, and we showed that they were there and important to us, but we had them outside of the boundary."

Regarding the actual assessment, much preparation was applied before the assessment took place. "The assessors reached out," she says. "They were like, 'Here's the collaboration tool. Here's how we're going to use it. Let's schedule a time to get you and your team and folks together to make sure that it works, that you guys are comfortable with it. Here's the control families. Here's how we're going to talk to them on each day.' What we did in advance is we had a matrix of our points of contact internally for the controls, but it was older, and we fine-tuned it so that we went through all 110 controls for DIBCAC. And we made sure that we had a point of contact, whether it was the network lead, the server, shared services, the SOC, which team it was, and then also looked to say, 'Okay, so just because this is a network type control, we have our network director, is he really the one who's going to provide the show-me or how do you do this, or is it somebody else?"

Howland added that they had their artifacts organized in order and labeled by control. In fact, they were labeled by CMMC and NIST 171. "We set up times on everyone's calendar and we blocked off the time. The DIBCAC assessment is about a week. It's less. The first day is an in-brief from the DIBCAC, and it's also an in-brief from the company. I'm going to kind of go back and forth here and go through the timeline and talk about how that came about. So as for prep, they provide a list of things that they'd like to see in advance. They're not always very specific, but that talks to, and you'll know what it is to provide to get there."

She advises to gather all necessary supporting information or artifacts such as standards, policies, governance document, network diagram, etc. Get all this ready and packaged up in advance of the assessment and submit it. They also prepared a PowerPoint as a means of responding to what the assessors wanted to speak about. She said the first day was a reading day. The assessment team takes all the documentation that you provided and looks through it.

Each day assessors had their own internal meeting to discuss how the day went. Then internal teams met to discuss how they did. They conducted a "hotwash" with the assessors in the late afternoon and went through everything from the day. Assessors would flash up the sheet of all the controls and you'd see all the greens or where they had checked things off. If there was anything to discuss or any questions, they'd made you aware of it that moment, that day.

You knew of any problems in advance. At the debrief at the end, there was no surprise. "It was really everything we were aware of every day," she explains. "And the score was provided. They'd talk about how the score would be calculated. There had been some discussions where there's not really a passing grade. They did explain how it can be, very negative. But they provide that. If there's any findings, they will talk to what the finding is, and that's really it. They don't tell you how to do anything, how to fix anything, just if they had any findings. And then they provide a formal report, which they have up to 60 days to do."

They had the formalized report in about 45 days post assessment and there were no real surprises as the earlier meetings covered any red flags or negative scores on controls.

Overall, the town hall meeting provided a first glimpse at what a real cybersecurity audit looks like. Some in the CMMC world and the defense industrial base have been through other audits, SOC audits or FedRAMP or something similar, but for many the DIB, their first experience will be either their CMMC audit or maybe a DIBCAC audit ahead of that.