**Meeting Notes - NeoSystems Town Hall Meeting – May 12 2021**

**Attendees:**

 *Mr. Ed Bassett, CISO, NeoSystems Corporation*

*Mr. Bob Metzger,* attorney in the Washington, D.C. office of the San Francisco based law firm Rogers Joseph O'Donnell. He is also the co-author of the MITRE “Deliver Uncompromised” Report.

Bob Metzger is an attorney with the law firm Rogers Joseph O'Donnell. The firm’s Washington DC Office is focused on government contracting. Metzger also co-authored the MITRE “Deliver Uncompromised” Report which was released in 2018 and one of the initial sparks that led to the CMMC program of today. He also served on the defense science board task force that produced the 2017 Cyber Supply Chain Report. He is very well informed on issues of supply chain risk and cyber threats which he applies that to his client base today.

The meeting began with Metzger discussing our current environment and recent events that have shown us that the threats that adversaries deliver are different in vector or method, and in consequence, than where CMMC has focused.

His take on CMMC is that it extends the present DFARS focus upon the protection of a network perimeter that tends to look toward the security of on-premises systems with the principal goal of protecting the confidentiality of certain types of information – controlled unclassified information (CUI). He states that the objective we're trying to achieve is to prevent the ex-filtration or loss or diversion of sensitive information, CUI, or intellectual property. He notes that adversaries have other vectors to pursue and other methods to pursue and other consequences that can follow.

He mentioned the Solar Winds security breach and explained that supply chain attacks can come, not just through cyber-IT or network connection, but can come through even trusted sources. They can come in ways where the national origin of the attack is disguised by having a facilitating US infrastructure and other areas of supply chain vulnerability, which can have physical or cyber consequences include cyber-IT against manufacturing or operational technology. These vulnerabilities can take place within firmware, software, and hardware. It’s important to be aware of vulnerabilities to sources of material and their quality, and to the logistics organizations employed to stage and deliver goods and services. Additionally, he says we must be thinking about the risks that adversaries will use, what they learned about our workforce, and methods of social manipulation to subvert, or potentially to turn employees into insider threats.

Metzger emphasizes this presents a huge span of challenges and problems. “I wish that I were just speculating about things that might occur and worrying about possibilities that won't happen,” he says. “But every aspect of what I just discussed is in the real world. And we've had recent, almost weekly, painful examples of these problems.”

He adds that CMMC has many values, and it has propelled the industry to get smarter and to work more. It covers only a portion of the broader threat landscape. "We're going to need to think about ways in which industry can concentrate its resources, human, technical, and financial, to get the most effective results accomplished against the broad reach of these threats," he says, "and it could be that we might want to change the relative priority of CMMC and information confidentiality protection, so that we don't spend too much resources sort of on one thing and neglect other things that could actually have more consequence.”

Metzger says companies have invested in being part of that ecosystem, but he finds it peculiar that we are creating a new method and an all-new infrastructure for assessment and accreditation, when there already are entities who are very capable of, and have their own regimes established for assessment, certification and accreditation.

“As I look at CMMC on the ground now, what I see is that the scale of CMMC's requirements potentially reaching 20, 30, or a thousand or more companies for that level three, it's extremely big," he says. “And we're finding that there's this funnel of the availability of accredited assessors, which is extremely small. We're not going to be able to achieve the objectives of CMMC unless we find a way to make the assessment and accreditation validation mechanism kind of hit the scale of the industry to be affected.”

Metzger says an idealized element to the CMMC maturity model and to the articulation of the program and the present plans as expressed by its leadership. "There's this idea that we're going to take on 20,000 companies and do assessments and require certifications for maturity level three,” says Metzger. “And then we're going to take on another 300,000 just to make sure that they properly protect that federal contract information. You've got to be sensitive to, let's call it the value proposition. You have a finite amount of resources, human, technical, and financial. You have a diverse array of problems. You want to be at least sensitive to whether the theory that you articulated and the methods that you employ to pursue that theory are going to produce results that are proportionate or commensurate to the investment and that the central purposes of the exercise.”

Metzger added that the most at-risk is that part of the defense industrial base that that works at [CMMC] level three, which is the same group that's required to meet DFARS 171 now. “I think we would do a huge amount if we could actually have confidence that, say, 20,000 companies really do satisfy not just 171, but those extra 20 mostly policies that are in CMMC maturity level three,” he says. “I think that would be a great accomplishment. Getting that done is going to be incredibly difficult. This is a complex machine with so many levers, gears, interconnects, and the like. And what we're finding is that if any part of it sort of goes wrong, it’s a problem.”

Metzger says if you don't have enough assessors, (and those you do have get behind schedule), if you don't have enough reviewers of the assessors, if you don't have enough companies that are not comfortable enough and they don't understand how much they have to cover or what they have to do, and if anything goes wrong in the system - it doesn't work.

Regarding CUI, he says his perspective maybe viewed as controversial. I don't think that all CUI is created equally, he says. “I recognize that there are categories and subcategories of CUI and the NARA rule, and I've read it, and I view that CUIs essentially are various types of information which the government must protect because government law, regulation or policy tell the government it has to protect them. And we have this peculiarity in the 7012 rule that sort of, we've gone outside that boundary of things that the government has to protect and suddenly said, 'You contractors have to protect some stuff as well."

Metzger believes it's the government's job to identify CUI, to designate it, to tell you if you're using it, and to tell you when you're supplying it. "I appreciate that the purposes of 7012 and CMMC are broader and important,” he says. “Those purposes are not just to protect that narrow category of information that has a distribution statement. Those purposes are to protect information which you do not want our adversaries to have, which you do not want to have compromised, which you do not want subjected to ransomware, you do not want to have corrupted, you don't want to have denied.”

The meeting wound down with some audience questions and commentary by Mr. Metzger and Mr. Bassett.