**Meeting Notes: NeoSystems Town Hall Meeting, April 14 2021**

**Attendees:**

 *Mr. Ed Bassett, CISO, NeoSystems Corporation*

*Mr. Mark Montgomery, Senior Director of CCTI and Senior Fellow at Foundation for Defense of Democracies (FDD) and Executive Director Cyberspace Solarium Commission*

Mark Montgomery served as the executive director of the congressionally mandated Cyberspace Solarium Commission, where he remains a senior advisor. Previously, he served as policy director for the Senate Armed Services Committee under the leadership of senator John McCain, coordinating policy efforts on national security strategy, capabilities and requirements and cyber policy. Prior to that, Mark served for 32 years in the US Navy as a nuclear trained surface warfare officer retiring as Rear Admiral in 2017.

Mark Montgomery opened by saying that he believes the right people are in the right jobs to vault cybersecurity programs upward, including into the White House, where it must be. The folks in his organization have not only the right skill sets, but the right relationships and he spoke optimistically about the way ahead for cyber – mostly.

He did mention that the prioritization of cyber is high at organizations such as CISA, NSA, and military organizations, but is falling further down as a budget priority at many federal agencies.

He spoke specifically of Mr. Chris Inglis, who was recently nominated to fill the National Cybersecurity Director (NCD) position (he still must be approved). He is in favor of Inglis for this position and believes it will enable cyber policy to find its way inside the White House as the reporting chain is directly to the President. It also gets it inside the final budget decision-making process and the initial incident response process, and even the campaign planning process.

"Direction to fund cybersecurity at a certain level's a top-down thing,” says Montgomery. “It has not happened as a result. With 108 federal agencies and departments out there, most of them do not see cybersecurity as a top one, two or three priority with exception of CISA, maybe NSA, [and] Cybercom.

He says most see cybersecurity as an element of the military. The majority are putting cybersecurity lower on their priority ranking. An NCD can emphasize to agencies that cyber can’t wind up on the chopping floor and that cybersecurity is high on the President’s list of priority issues.

In the last budget cycle, Montgomery says there was a $110 million increase for cybersecurity initiatives - about 5%.

“I fully support 5% but I would also say I fully support 15 to 20% as the right number," Montgomery says. “In general, non-DOD federal agencies had a 16% increase in budget. The president said, very clearly, cybersecurity is a priority. A priority shouldn't get 5%, it should get between 15 and 20%. They could easily spend that effectively on the other half of their mission meeting their new missions and their existing gaps and building a better public-private collaboration.”

Ed Bassett did bring up Solar Winds and Microsoft Exchange security breaches. Montgomery commented that over time there will be an increasing availability of malicious cyber tools available to actors and such tools will increase exponentially. “The inter-connectivity of our systems has increased exponentially," Montgomery says. “Our investment in cyber-defenses has been linear, kind of on a low glide slope. When your risk drivers are exponential and your risk mitigator linear, you've got a lot of risk. I think most of us saw this and I think this has been demonstrated by both these events, but people knew that. Now what's changed is I don't believe the $650 million for CISA, the billion dollars for the tech modernization fund, would have been in the COVID legislation, if it weren't for SolarWinds and Microsoft Exchange.”

Ed Bassett then shifted the conversation to certification and labeling of IT products. Montgomery commented that the national cyber security certification labeling authorities is a provision that his organization continues to push. He is reluctant to say that if certification and labeling had been solidified earlier that it may not have prevented the SolarWinds breach – necessarily. But it would push a broader raising of the overall cyber ecosystem. It would certainly make it easier for those in small or medium-sized businesses to know that the software they're purchasing has the necessary security embedded in it.

Ed Bassett then raised the issue of CMMC certification, but notes that in the recent security breaches, there were thousands of persons involved. Could a certification program had thwarted or prevented some of the breaches. Montgomery says that these were more espionage attacks than cybersecurity attacks.

“This was not a cyber-attack and that matters,” says Montgomery. “It matters in how we respond. It doesn't matter how you defend though. And the idea is you do have to build better defenses. I think a thousand is a lot, that's a lot of APTs strung together. Should they be able to do that? Yes. Should a company be able to do that, even a large American company? No. And should Jim's dry cleaner down the street be able to take it, of course not. Your PII data there is gone if an APT decides to target that."

When it comes to cyber security, Montgomery says there's three legs to the stool: technology, people and processes. Technology is covered by certification labeling authority and the identification of appropriate software to use. For the processes, it's about getting out good business cyber hygiene. This leads to things like how do I do my domain registration? How do I approach DMARC? Do I make the right security decisions at the kind of IT administrator level and how do I log? How should one implement the processes? And then finally the people and in some ways, the least expensive and most effective investment; he notes that it takes persistence to train people.

In concluding, Montgomery says it's important to get inside your system. If you can't, you need a third party to do it. He adds that another important takeaway is to focus on business cyber hygiene training for your workforce.

He poses the questions: “How are you setting up your systems? How are your people operating on your systems? And this isn't just everybody with an administrator login?

They and those who can influence that decision-making must be trained properly to make the right decisions. If you can get right inside your system, and properly train those who are not only administrators but also decision makers, (one of which is expensive and one of which is cheap) you're going to have a significant, positive impact on the cybersecurity of your platform.