NCSC & ONCD Podcast Transcript

October 26, 2022

Jeanette: Hello, and welcome to the National Counterintelligence and Security Center--or NCSC--Supply Chain Podcast series. These podcast highlight the work of supply chain experts and practitioners from government, industry, research, and academia with the goal to share information on supply chain security topics. Through these quick segments, we hope to bring awareness of supply chain security and efforts to prevent foreign attempts to compromise the integrity, trustworthiness, and authenticity of critical U.S. supply chains.

[TIME: 00:00:32]

My name is Jeanette McMillian and I serve as the Assistant Director for the National Counterintelligence and Supply Chain and Cyber Directorate. Joining me for this podcast is Principal Deputy National Cyber Director for the Office of the National Cyber Director, Ms. Kemba Walden. Ms. Walden brings a wealth of public service and private sector experience to this role, including her work as assistant general counsel for Microsoft's Digital Crimes Unit and her service at the Department of Homeland Security, where she served as a cybersecurity attorney for the newly created Cybersecurity and Infrastructure Security Agency, or CISA.

[TIME: 00:01:09]

As this podcast of being recorded during October, which is National Cybersecurity Awareness Month, we were honored to have Ms. Walden join us to highlight some of the initiatives that the Office of the National Cyber Director has taken on during its pilot year and those efforts they will be leading in this upcoming year, as they seek to do more cyber awareness security efforts. So, for this podcast, we hope you enjoy this cyber supply chain. Conversation thanks for listening.

[TIME: 00:01:40]

Jeanette: Thanks again for participating in this podcast with me.

Kemba: Thank you for having me, Jeanette.

Jeanette: Yes, so, ONCD Director Chris Inglis joined us for Supply Chain Month in April. We were so excited to have him, and he started to talk about the startup of ONCD and the vision of cyber that he had for the office--but, more importantly--for the nation. So, one of the first things he was going to do is bring in the talent, and so I understand that that was one of the reasons why he sought to make sure that his office with well staffed.

[TIME: 00:02:14]

So, the first thing I wanted to ask is, you know, if you could, just please share with us your expertise and why you were drawn to support Director Inglis's vision.

Kemba: Sure, I'll start with supporting Director Inglis's vision first and then work backwards, explain how my expertise meets that vision. So, we might cast the vision differently, but we get to the same place. I view that our North Star for the office--the reason why I do cyber--is to help communities thrive and prosper in this interconnected world--

[TIME: 00:02:45]

That's it. Cybersecurity's a means to that end. So, given that's the North Star and that's the vision that Director Inglis presented to me, it makes sense that I'm in this role. I started my career focused on development--international development, specifically--but come full circle now, realizing that development doesn't really take place unless communities feel secure. That's true in the physical world and that's true in cyberspace, and so I feel that that is my role here.

[TIME: 00:03:15]

That's the talent that I bring.

Jeanette: Awesome, awesome. So, no, that is that's definitely one of the things that we're looking here, in terms of the National Counterintelligence and Security Center's goal with regards to how cyber security and, more importantly, how we're positioned in the world to ensure that those like-minded nations are in that secure space as we live with the digital age. It is definitely very interesting. With that in mind what goals has ONCD achieved in the first year towards building that more secure community and also what are the goals for the upcoming future?

[TIME: 00:03:54]

Kemba: So, we have four measurable outcomes that we're seeking to achieve. The first is driving federal cohesion. As you know--

Jeanette: Yes.

Kemba: Working at ODNI, we have multiple agencies that are involved in or, ah--objectively performing in cybersecurity across twenty-three or more federal agencies, so we're here to drive federal cohesion so that you don't have to have a PhD to understand how the federal government works in the space. Just as important, we're here to drive public/private collaboration, which is something evolved from information sharing.

[TIME: 00:04:32]

It's really driving insights from all parties in order to be able to have actionable outcomes. It's professional intimacy as opposed to information sharing, the third and maybe least sexy, would be we have a performance metrics responsibility, really aligning resources with aspirations so that we don't have unfunded mandates and that we drive capital expenditures in cyber-security.

[TIME: 00:05:02]

And then finally, this sort of the core of our work is driving future resilience, making sure that what we do have in cyberspace was at once defensible, but any residual risk after buying down that defensible risk is resilient, so, in the technology and the people in the processes in cyberspace. So those are our four achievable outcomes that we're trying to achieve.

Jeanette: Fantastic.

Kemba: We're doing that now, we will do that into the future.

Jeanette: Awesome. No, that is--those are so awesome, and I love the fact, though, that metric is also very, ah, tangible and we're where--

[TIME: 00:05:38]

You have to understand that if you're going to achieve something, you have to measure it, so pushing those metrics is absolutely ideal. From NCSC's perspective, but, more importantly, from the greater ODNI. How is it that we can better support and also to help achieve those goals that you guys have set out for the next few years?

Kemba: Well, ODNI, obviously, we have a great relationship with the Intelligence Community, as you know risk is some combination of threat, vulnerability, and consequence

Jeanette: Absolutely.

[TIME: 00:06:09]

Kemba: The IC is really--has developed expertise in developing the threat model, right? Explaining to us what the threats are so, for example, as we're looking across industry and other partners and identifying risk and helping the public sector and the private sector in academia drive that risk down, it is important for them to understand threat. We look to the IC to help us help them understand threat and it's really the marriage of threat and vulnerability then that explains risk so that those in industry and those in the federal government can make the appropriate

[TIME: 00:06:50]

investments in order to ensure that they're able to buy down that risk and that they're able to make the residual risk resilient. That, plus on the very practical side, we have great, great detailees in our office from the Intelligence Community that really add to the value that we're able to bring to the entire cybersecurity community and we're grateful for that, so I just want to make a plug to ODNI. We would love to have more.

Jeanette: Yes, yes. No, I think there were so many people that volunteered--it was not even a volun-told situation, because the mission is so important, and under your leadership as well as Director Inglis, I think there were, there were so many people that wanted to go so I'm so glad we were able to have those folks that are there and and you're absolutely right with regard to how to to build that bridge with regards to that threat information and one of the key aspects that we do here for the DNI is indeed developing that supply chain security risk information, as well as the cybersecurity information, and also counterintelligence security information, and, in fact, on behalf of the DNI, we actually chair the DNI Supply Chain and Counterintelligence Risk Management Task Force and that task force is aimed at providing that sort of information that is actionable and information--getting that outside of the Intelligence Community,

[TIME: 00:08:11]

you know, at an UNCLASSIFIED and actionable level to make sure that that information is actioned for federal departments and agencies, those that are in critical infrastructure sectors and then also making sure that those risk management agencies can have that good dialogue with the private sector for securing our supply chain risk management efforts within the cyber domain, so, so glad that you had mentioned those things, but um, and we've taken great strides within the task force. But specifically, is there anything else that we would want to do in terms of information sharing that you can see?

[TIME: 00:08:45]

Kemba: Well, I think a pivotal moment for us, but in the cybersecurity community that sort of re-shaped how we think about information sharing was frankly, uh, the onset of the Russian aggression against Ukraine. We were able to get the actionable information with, with the extraordinary help from that intelligence community to those that can take action. So, for example, we collaborated with the financial industry, knowing that we were going to place sanctions on Russian entities in advance of their aggression or at the onset of the aggression.

[TIME: 00:09:19]

We thought, perhaps, there might be some retaliatory effects on the financial services community, so we were able, with your help, to share actionable important information and get it into the hands of those that could actually take action, and I think that's the paradigm shift that we're working with now that's evolving, so that we understand we're not--we meaning the U.S. government--are not in this by ourselves. We are not capable of doing this by ourselves,

[TIME: 00:09:51]

and it doesn't make sense to hold on information that we cannot action as effectively as others. So that's, I think that demonstrates a paradigm shift for us.

Jeanette: Absolutely, no, that that is an excellent segue as well, because I think that paradigm shift, you can see a little bit in the new National Security Strategy that was just published a few weeks ago, and I, for one, was super excited to see how that the NSS incorporates cybersecurity, and I understand that a lot of work has been ongoing.

[TIME: 00:10:23]

I'm not going to ask you to plug your strategy; I know it's still in the works, but if there's any highlights that you can share with us along the way in terms of making sure that that journey is mirrored because also for NCSC on behalf of the nation, we have a requirement to build our national counterintelligence strategy too, so just making sure that all of those things flow together, what are those things that were highlighted in the NSS that would be beneficial for folks listening out there.

Kemba: So, when the National Cybersecurity Strategy comes out

[TIME: 00:10:55]

and that--we can't anticipate when that'll happen--

Jeanette: Sure.

Kemba: But you'll see some, some of the same framing, right? So we're looking at a decisive decade. The strategy is forward-proactive forward-leaning, proactive in tone. So it describes an Internet that we imagine that we are securing, right? One that reflects our Democratic values, one that empowers the economy, one that protects privacy and so on,

[TIME: 00:11:26]

and we are here to make sure that cybersecurity delivers on that promise of Internet.

So you'll see several pillars and that you wouldn't ordinarily see in a strategy, but there are two overarching themes that I want to want to touch to, and this is really the work of the nation as it's the National Cybersecurity Strategy, not mine, right, not Chris Inglis's, but the National Cybersecurity Strategy. The first is that we need to re-think how we allocate risk--

[TIME: 00:11:58]

Cybersecurity risk, if you think about it, is really borne by the end user right now, small and medium businesses, my daughter can click on a cat meme and cause a national security incident, and that's just wrong.

Jeanette: Right.

Kemba: We need to re-think risk so that we shift from small and user to the enterprises, including the federal enterprise that is able to bear that risk and buy it down

Jeanette: Correct.

Kemba: And then we have to think about resilience and what we do with that residual risk, right? And cyberspace,

[TIME: 00:12:31]

as you understand, is not just a technology, though that's important, but it's people and it's processes, and so you'll see all of these elements of cyberspace and the drive for resilience in that space throughout the National Cybersecurity Strategy.

It's really exploring what investments do we need to make now for that decisive decade. The second piece that you're going to see--

Pretty clearly and the strategy has to do with public/private partnerships, the investment we need to make there acknowledging that this is an all-of-us proposition not just a some-of-us proposition not a division of responsibility, but a cohesive all-of-us proposition such that and, as the director would say, you would have to beat all of us to beat one of us.

Jeanette: That's right. Right.

Kemba: So those, that's the tone of the Cybersecurity Strategy as we've crafted it.

Jeanette: Oh, no, those are great great highlights-

[TIME: 00:13:30]

And I definitely want to hit that mantra with, "If you got to beat all of us to beat one of us." No, that is absolutely great, thank you so much for taking the time to give us those kind of highlights and overview, and I think one of the things that we wanted to take away as well is what are those in cyber needing to do in terms of cyber professionals, in terms of these strategies, how should they see themselves in terms of being able to bring that strategy down to the tactical level in terms of what a cyber professional needs to be concerned about again being in this for the, for the next decade.

[TIME: 00:14:05]

Kemba: Yeah so like, I said before, first it's helpful to understand how we view cyberspace right? It's the technology, the hardware/software, it's the people that are in cyber. They're not under cyber, they're not above cyber, they're not on the side of cyber. They, they create the Internet that we're using and they use cyber. They use the Internet and then there's the processes, right, who's responsible for what? Who's guarding the gates. We need to address vulnerabilities in all three pieces--

Jeanette: Correct.

Kemba: In order to enable a free and open interoperable Internet, right?

Jeanette: Right.

[TIME: 00:14:40]

Kemba: So the people question is what you've asked about--the national cyber strategy will be published at some point soon, but we're right now working on the people piece of it, and we will have a national cyber workforce in education strategy really targeting the question that you asked. So they're, something like seven hundred thousand unfilled jobs right now, nationwide with the word cyber IT in them--

In my view, coming from a national security background, that's a national security problem,

[TIME: 00:15:10]

but it is also an economic development problem in our country we must address, and so we're looking at opportunities to address that. But then we have to also think about those professions that implicate cyber: Accountants, lawyers like me, members of the board of directors. They implicate cyber and we need to lift cyber awareness in those spaces. But then, what's the pipeline coming from? It's coming from all of us, right?

Jeanette: Right.

Kemba: So that if we're looking to build resilience, for example,

[TIME: 00:15:41]

we have cars, for example, consumers will buy a car for the ease of the car. They're not thinking about having to add on air bags and anti-lock brakes and a seat belt.

But consumers know that they must buckle the seat belt.

Jeanette: Right.

Kemba: Must follow the road signs. They're not the ones creating that. That's where we're trying to drive cyber so that once we buy down that risk, we are also looking at all of us that are that are working and functioning in this interconnected society, right?

[TIME: 00:16:12]

Our thermostats are connected, our refrigerators are connected. Our children are using iPads and other devices in school. How are we educating the general public about cyber and their role in that space?

So we're really working on a strategy that focuses on those--I view it as concentric circles right?

Jeanette: Nice.

Kemba: Those with cyber in their job, those that implicate cyber and then the all of us, right? Kids, grandparents, all of us--

Jeanette: Yeah, no, no, that’s a great answer, and

[TIME: 00:16:42]

it’s very interesting, and just in terms of the generational, you know, divide there, uh, whenever there’s, you know, something going on, my, we, we definitely need to make sure that our children are aware of those things in that it’s not just about the fun and games, but it’s how they're protecting their own data--

Kemba: Right.

Jeanette: As as they go forward in their in their one-hundred-percent digitally connected environment. They cannot unplug, right?

Kemba: Oh, no, they can't.

Jeanette: So it’s definitely one of those things, so staying on the cyber professional track for just a second, CISA Director Jen Easterly pledged to increase the number of women in cyber to fifty percent by 2030. An ambitious goal, and one I certainly hope to help achieve by making awareness and also making sure that we were highlighting this need for additional cyber professionals

[TIME: 00:17:29]

to kind of close that gap in terms of skill sets and then also close that number of open positions within cyber and IT. ONCD has certainly helped with the initiatives. I think you placed that in July, with regards to meeting that goal. If you can, please share some of those initiatives in terms of the cyber summit workforce that was also held out there and then how we can still continue to help achieve that goal from it. ONCD's perspective.

Kemba: Yeah, so I wholeheartedly support Jen's mission to increase--right?

[TIME: 00:18:02]

I'm a pawn in that game. I’m happy to be so.

Jeanette: That's right.

Kemba: Cybersecurity is, if you think about, is a complex area in a lot of ways and it requires complex, um, response. Meaning we need diversity of thought, we need a diverse workforce in many ways, right? Gender is one of those very important ways that we need to to diversify the workforce. Neurodiversity, um racial diversity, international diversity, diversity of thought, political diversity.

[TIME: 00:18:34]

However, you want to define diversity. All of us have to be in this space in order to be able to secure it, right? And we're looking to secure it, so that the Internet is able to deliver those things that we expect the Internet to deliver.

Jeanette: Right.

Kemba: Women is, we are a large part of this conversation, we're a large part of the equation and we've--our office in particular--has shown that it takes an office that looks like America to be able to

[TIME: 00:19:06]

deliver the outcomes that we're seeking to deliver. That's just true.

Jeanette: Right.

Kemba: And I am all on board with Jen's mission. I'm right there with her. I teach the Cybersecurity Badge for my daughter's Girl Scout troop.

Jeanette: Fantastic! Fantastic! It's not just about cookies.

Kemba: It's not just about cookies. That's right. But no, it takes all of us to defend cyberspace 'cause the space is complex, and so we need a diverse set of thinkers to be able to achieve what we need to achieve.

Jeanette: Absolutely absolutely.

[TIME: 00:19:39]

Well, no, I can't thank you enough for spending some time here with us and with our listeners. Kemba, thanks again for joining me for this collaborative podcast opportunity, and I hope we will continue to enhance our collective mission priorities to raise cybersecurity awareness to secure a more resilient, cyber supply chain.

Kemba: I appreciate it. Thank you for having me. This is been a pleasure.

Jeanette: Awesome.