Kevin Minor: 0:02
Greetings and welcome to the NASPO Pulse, the podcast where we are monitoring issues in state procurement. We've got our finger on the pulse. I'm your host, kevin Miner, and Josh is out this week in Arizona at NASPO Law Institute slash STCC that's State Training Coordinators Conference so we hope he's having a good time there representing. Fortunately for you, though, I am still in the studio. I'm taking the pulse. We're good to go. And, man do? We have an episode for you today? We are talking about cybersecurity. All right, don't run away. Don't run away. No, no, this is going to be a good one, I promise. We're not just talking about changing your password, although if you haven't done that recently, you probably should. No, today we're talking with two titans in their field. We're talking with Russell Porter, a senior executive for the Office of the Director of National Counterintelligence and Security Center that's NCSC, and they're a valued partner of ours. And we're also talking with Dugan Petty, former NASPO Value Point Cooperative Contract Coordinator, former NASPO President, former CIO, former CPO, former NASIO President, and the list goes on and on. We talk with Russ and Dugan about NCSC and NASPO's relationship. What's unique about government IT and the threats facing digital government, common government IT service or goods that have been targeted in the recent past, how CPOs and their staff can mitigate supply chain risk. And you guessed it much, much more.

Kevin Minor: 1:45
You do not want to miss out on this conversation. You got questions, comments. We'd love to hear from you. Email us podcast at naspoorg and if you haven't already, you make sure you subscribe to us on Apple Podcasts, spotify, google or wherever you get them. Sweet listenings. Check out the blog pulsenaspoorg and catch up on some procurement articles written by your very own NASPO staff. Let's take the pulse. You are a senior executive at the National Counterintelligence and Security Center, which is one of the three national centers within the Office of the Director of National Intelligence. Can you briefly explain what the NCSC is and your responsibilities there?

Russell Porter: 2:30
Sure, and first of all, kevin and Josh, thanks for the opportunity to join you today, and I'm honored to be with Dugan.

Russell Porter: 2:38
Ncsc, the National Counterintelligence and Security Center, leads and supports the counterintelligence and security activities of the entire US government, and so we produce, for example, a national threat assessment of the foreign intelligence threat. From that, we produce for the White House a national counterintelligence strategy for the United States that's signed by the president, and we also provide outreach to US entities that are at risk of foreign intelligence penetration and we issue public warnings regarding intelligence threats to the US. My responsibilities at NCSC include leading our strategic partnerships and outreach efforts with critical partners like you, listeners, and to help partners understand today's foreign threat to the homeland in fact in the homeland and what they can do about it. Before I came here to NCSC and the ODNI in 2010, I spent more than 30 years in local and state government, where I served as a law enforcement intelligence executive who provided insight what I hope is indispensable insight to senior state and local government executives, governors, lieutenant governors, homeland security advisors and so on.

Kevin Minor: 3:51
Wow, so just a little bit of experience there.

Russell Porter: 3:55
A few years, yeah, something near a little over 40.

Kevin Minor: 3:59
Wow, okay, great. And Dugan, can you tell us just a little bit about your role as a cooperative contract coordinator with NASPA ValuePoint?

Dugan Petty: 4:07
Yeah, sure, thanks for having me on.

Dugan Petty: 4:09
It's great to be here and looking forward to this conversation with Russ.

Dugan Petty: 4:14
I am a cooperative contract coordinator for information technology and communication technology projects at NASPA, valuepoint does. I kind of came to that role when I first joined a ValuePoint and my effort with ValuePoint was really to join to help create and work with Utah to support them in their procurement of a cloud solutions RFP. And then over time my role changed to a cooperative contract coordinator and I've really tried to work to support the coordinator who is really supporting the lead state and the contracting team, and work with the lead state and contracting team to kind of understand the IT perspective for our purchases. Before I retired from Oregon State Government I spent six years as Oregon CIO, so I have a kind of an understanding and background and experience with deploying technology at scale at state level and have a relationship with many of the NASEO members. So it gives me sort of a unique perspective that I try to bring to NASPO Value Point procurements to make sure that they are viable procurements for the states that are using them.

Kevin Minor: 5:48
Right, right, and you're kind of a jack of all trades, so to speak, in that area. Master of all.

Dugan Petty: 5:53
Yeah, well, that's probably a good description, he's being mild Jack of all trades yeah.

Kevin Minor: 6:00
Yeah, absolutely.

Russell Porter: 6:14
So, russ, how do you and Dugan know each other? How have you worked? Because I want to talk about the relationship between NCSC and NASPO because of my state and local background, and in February of 2020, ncsc I mentioned earlier the National Counterintelligence Strategy released the current strategy, february of 2020. No-transcript those five strategic objectives in that strategy, which says there are more threat actors using more sophisticated and aggressive methods and attacking more targets in the homeland, says we need to do five things First, protect our critical infrastructure. Second, counter exploitation of the economy. Third, defend our democracy against foreign influence and you see these things in the news all the time Fourth, counter foreign intelligence, cyber and technical operations. And then, fifth, reduce threats to our supply chains. And so I knew that it was important for our community, our counterintelligence community nationally, to have a relationship with procurement professionals. And as I looked around, I knew that NASPO was someone that we needed to reach out to, and was so glad that we found such a great partner with Dugan and the whole team, olivia and others at NASPO.

Josh Descoteaux: 8:16
And Russ. I have a question to that With all of your experience in the past 30 years, what have you seen change? What have you seen change with the threats and with the contracting now and the supply chain efforts and the strategy to mitigate those threats? Has that been a newer, emerging kind of strategy related to procurement or has that been around? And if it's been around, what's changed?

Russell Porter: 8:39
Yeah, that's a great question, Josh. So it has changed. At least, certainly my understanding of it has changed, and maybe, if I could explain it in this context, as a state and local government official, I really never, I mean, I paid

attention to the global security environment and the threats out there, but I really didn't focus on and I think that that's a change for today. I think people have to focus on it at all levels of government and in the private sector, and so here's how I've tried to approach it myself.

Russell Porter: 9:14
You know, we all kind of get the concept of war, which is powerful military forces that are fighting tank to tank and battleship to battleship and fighter plane to fighter plane and so on, and we understand peace, which is tranquility, the absence of war. But there's a third condition, and I think people will recognize much of this today. It's often referred to as the gray zone or hybrid warfare, asymmetrical warfare. And here are the tactics that exist in the gray zone Election meddling, assaults on critical infrastructure, disinformation campaigns, spreading propaganda and sowing divisiveness in a society, undermining confidence and trust in democratic institutions, whether it's through a hack and leak type operation and then releasing the information that an organization doesn't want released, and so on, all of those we read and hear about those things in the news virtually every day.

Josh Descoteaux: 10:16
And so that's why this national CI strategy is a part of this right.

Russell Porter: 10:19
It's because it's so important for people to understand how supply chain and the contracts we have with third party vendors and suppliers and so on. It's really important to pay attention to that in the current environment.

Kevin Minor: 10:36
And so what's unique about the government, it and the threats facing digital government?

Russell Porter: 10:44
I mean, in some ways it's not unique because it's out there as a target. The foreign adversaries see it as another target. But I want to disabuse people of the notion that local or state or federal governments are not of interest to foreign intelligence threat actors. You know, it's not just the Department of Defense Dukin and I have talked about this it's not just the Department of Defense or US intelligence community issue. Things are especially in the aggregate things that data that's held by local and state governments is of interest to foreign intelligence adversaries Voter registration systems, driver's license information, employee rosters, personnel records, email systems and so on. All of that is of interest when we think about war, peace or the gray zone, the gray zone tactics that are being used currently by our foreign intelligence adversaries.

Josh Descoteaux: 11:50
And Dugan. So, with all those threats that Russ just had alluded to in terms of public contracting, public procurement supply chain, specifically in the IT space, what can the public procurement sector do to mitigate those risks?

Dugan Petty: 12:10
Well, I think that the public sector, the public supply chain sector, just like any supply chain sector, the procurement people actually, whether they know it or not, they're on the team and they have to be on the team because this is something that's in their wheelhouse, that they control that procurement process and those contracting processes. Those are things that they can control and really have a responsibility to make sure that they're protecting their state's interests and their clients' interests as they buy forms. So I think there's a role to play as the contracting community. The procurement community develops RFPs, makes selection processes and addresses in their contract something that Russ mentioned third-party risk, and we'll probably get into that a little bit later in more detail, but that's really critical. So there's clearly a role to play and, frankly, if the procurement office isn't on board with that, then somebody else would have to do it for them, because we now know that our contracting avenue has become a threat vector for attacks.

Dugan Petty: 13:32
You know SolarWinds. There's been over 3,000 articles published on SolarWinds. That's kind of amazing and the impacts with that have been really impressive. With that have been really impressive 18,000 customers unknowingly installed malicious code with a trusted supplier that is a good supplier, and so that's kind of shined a light on something that's been around, really a risk and a vulnerability. It's been around forever. It hasn't been exploited.

Russell Porter: 14:02
The only thing I would add to what Dugan said and I agree with him wholeheartedly is, yes, that this is an issue that's been around for quite a while, but we know that the threat actors are intensifying their activities and becoming more aggressive, and so this is almost a call to action, if you will, in the ways that Dugan has described.

Josh Descoteaux: 14:26
Absolutely, and it's a good conversation to have, just to have everybody aware of this, and unfortunately, I guess my question kind of came from my honesty of you know, has this emerged? Is this emerging? And the answer is it's always been here, but it's coming and showing up in very different ways and I think it's on the national stage, international stage now, in ways that it never has been before. Just as a general consumer, you're hearing this every single day now. So it's a trend. This is an opportunity to change. But are we late in the game? Russ, and you know, in terms of all of your experience working with cities, counties, working with cities, counties, municipalities, states, territories, how can, right now, we move forward? And Dugan had touched on this about you know it's a national, international effort to pull together. So, with your experience working with those entities, what's the strategy now going forward?

Russell Porter: 15:25
I mean, I think, for people who are and I'll call it at the tip of the spear Right, I mean the people who are the professionals that are in the procurement process, people who are responsible for hiring good personnel in your organizations, and that's all at the tip of the spear to address this threat. And so, recognizing that that you do own the solutions if you act and I've, having spent most of my career in local and state government, I'm always a little bit, I always raise my eyebrows at a a solution that's going to be projected upon me out in a state or local government from Washington, right, you always just say, well, I don't know if that's going to be projected upon me out in a state or local government from Washington, right, you always just say, well, I don't know if that's my solution for me, and so we're not that kind of an organization that has specific what do you do about this? We do have some basic steps at a high level that any organization can take to address this particular issue, but here's what we can offer. And it's not to say that every manifestation of these threats is coming from a nation state actor or a foreign intelligence entity, that's a non-state actor. But it is to say that those actors are increasing what they do. It is who we focus on, and it's why information sharing two-way information sharing is so important for us to make sure we're conveying what we understand that threat to be.

Russell Porter: 17:00
We know that the tools and capabilities of these very powerful, sophisticated, highly trained, well-organized institutions that commit these acts, those tools and capabilities are sometimes used by others, and so just good advice generally is to take a good risk management approach, as Dugan has mentioned already, to make sure organizations are resilient. Diversify your supply chains, for example. Incorporate security by mitigating the third-party risks that we've already mentioned. Create transparency in your system by identifying and prioritizing the protection of your most important assets, things that, as I mentioned earlier, some people think well, I don't have a dog in this fight. Well, of course you do, because your data is, in the aggregate, important to others. And then, finally, as I mentioned before, strengthen partnerships and information sharing. We know local and state governments don't have the capabilities of, say, the US intelligence community to understand the plans, capabilities and intentions, but we can bring, at a strategic level, that kind of awareness to this conversation. Briefly, what are some things that?

Kevin Minor: 18:22
they can do now. What's some diligence that they can perform now that might help to mitigate and be proactive?

Dugan Petty: 18:39
Well, I think the first step is to ask the question of do you need to establish a cyber risk management framework in your office and understand at a starting point what the half dozen elements of that would be? And then you should do kind of a high-level assessment, probably in conjunction with the state CISO, what your risk levels are with your suppliers, and that would give you some idea of where you want to go. Next. It could very well be that you have a cyber framework that you would apply to a half a dozen contracts, at least as a starting point, and begin to ask the supplier what kind of third-party risk management they're using so that you could rely on them, because basically we've relied on all of our suppliers and some have that and frankly, many of them will be way ahead of the state. So that might be low-hanging fruit and if there is an issue, at least you're beginning to look at it and start on it. The other thing I think is important to do is I would suggest that any CPO or contracting officer or contracts manager that's involved with particularly with IT software, it cloud, they should be taking a look at NIST's new cyber supply chain risk management revision. This is SP800-161. It has been upgraded very recently based on supply chain risks that NIST is seeing, and the new draft is out for comment. I think the comment period has been extended, but they believe that it will be out for a second comment later on. In last I saw would be September 2021 and their target for the final version of that is 2022. But that is a textbook in cyber risk management and third-party risk management, so I mean just going through that you'll learn a lot. Nist has put out a number of publications and a number of recent case studies and material in dealing with the cybersecurity supply chain and I think that that would be wise reading of somebody in every state procurement organization because there's a good chance. I talked to to state CBOs who said this is an issue that we're beginning to hear about and if we don't do something about it, it sounds like the legislature might do something about it. So I think if it's not on your radar screen, it probably should be.

Dugan Petty: 21:42
And these NIST documents, I mean there's really nothing better. They are tasked by the White House and by Congress to do this work. They bring in experts from around the country, including their own researchers, and it's really the definitive document. So using that and relying on this is a very simple thing to do, and while some of it is designed for federal agencies, that doesn't mean that you can't use it as a state agency, and so the principles and practices are largely the same.

Dugan Petty: 22:20
The other thing I think I'd like to mention here is that we've done with the National Counterintelligence Security Center. We've done a couple of webinars and we did a presentation to our leads group with Joyce Correll. She's just a whiz on this and wonderful and she's really been helpful. But she sets on a federal agency group working on federal contract language and in requirements to begin to address this, and she's offered to stay connected with NASPO on this issue. There's an opportunity for NASPO and NCSC to work collaboratively here to help share that and kind of incubate that information, and I think there's a great opportunity for us, and I think if I were a CPO still a CPO I would be very interested in understanding what's happening in that arena and seeing how that might apply to my contract documents.

Josh Descoteaux: 23:34
And Dugan real quick to get down to the procurement office level, the state procurement office level, when you had mentioned the NIST standards and then also looking into the third-party vetting of the contractors or prospective bidders. Are you saying in terms of an evaluation process, to integrate more of that in terms of a weight of an award of a contract and to almost put that into your processes as a larger weighted decision-making tool to be able to vet those contractors and make that a standard piece or a bigger piece of your evaluation process?

Dugan Petty: 24:19
Well, that's part of it. I would also put controls in the contract, very specific controls that would flow down to the

third party suppliers, requiring them to meet certain controls that are designed to protect the supply chain, resiliency and continuity and to keep nefarious code or bad code out of software, for example. I would put that in the contract language so that there's an expectation that if you're doing business with the state that you'll have that kind of risk management program. It doesn't mean that a problem won't happen even with that, but at least they're trying to do work to it.

Dugan Petty: 25:07
The other thing I think states have to consider the more and more I hear this is the idea of continuous monitoring. It's not good enough for somebody to say, yeah, at the time of award, I do this. How do you know that six months later that they have slacked off on this control or requirement to make sure that this certain standard is met? You don't know that and most states don't have the ability to do the continuous monitoring themselves. So that gets into a question of well, how is the supplier making sure of that? Are they having a qualified third party assess that? Is it a self-attestation?

Dugan Petty: 25:56
It's along the lines of requiring a SOX2 report as an example, but for some of these controls that continuous monitoring goes beyond what a SOX2 would do, because that particular control might not be in SOX2. And it is also similar to what StateRamp is beginning to do, but StateRamp is a specific cybersecurity regime aimed at cloud service providers, and so certainly StateRamp is looking at increasing that third-party risk management on the part of cloud service providers, but that only addresses cloud service providers. So if you're buying equipment or software or services that are not SaaS infrastructure or platform as a service then that's a different issue and you need to address that. But those similar risks can be there. So that cybersecurity framework SP 800-161, is designed not only for cloud but for any number of different supply chain cybersecurity risks.

Josh Descoteaux: 27:11
So you mentioned the collaboration between NCSC and NASPO. So what are the future plans of this relationship between the two entities?

Dugan Petty: 27:21
Well, we talked a little bit about the roundtable that NASPO convened with its partners and invited NCSC into that, and I thought that was an excellent discussion and it really made the point. I think a couple of points that came out of that is that this is one of these issues that isn't going to get solved within one functional area or one association's domain. It's really going to take all of us working in collaboration so that we're for one, we're working together on a solution, as opposed to we're diffusing all of our energies and going off in different directions. And two, it allows us to begin to develop, I think, a way of going forward that builds upon itself. We kind of talked about it as a crawl walk run strategy. We're not in a position to run on this issue. It is sort of a call to action, but we can't say and we have to do this and this and then we'll solve the problem. It's not that easy. We have to fully understand the problem, we have to understand the roles that we can take and we have to really assess what the best next steps are and then build on those steps to take the following steps. And so we're going to debrief later in this week, the NASPO team, get our notes together and then we'll come back and bring those partners all back together and, I think, propose some next steps that can have us working in concert towards making wise and prudent decisions to address these risks in a way that makes sense and is appropriate and is a responsible way to act. So I think that's going to open up a lot of opportunities.

Dugan Petty: 29:29
I think one of the things that we have yet to figure out but the benefit is so great not to I alluded to earlier is, while we don't have a seat in the federal supply group that is looking at this and developing contract terminology we have a good friend who does, and I think we need to create and NASPO probably is a good place for this the forum that we can understand what's going on there and contribute to that, maybe indirectly contribute to what's happening, but certainly learn from it and begin to apply that. The other thing that I think we certainly want to

figure out how to do and I think this is another next step that we could easily have a successful solution on and that is this idea of information sharing. Everyone I talk to and everything I read on this topic suggests that one of the important things, along with the third-party cybersecurity framework, to make sure that we're assessing risks and taking action to mitigate. That is, reporting on what's happened, some transparency around what the issue is and I think Russ has talked about that and I hear other people talking about it, and it seems to me that NASPO is uniquely situated to help play a really important role uh, to be that, to be that, um, that communicator, if you will, or forum, uh for those kinds of communications as it relates to the supply chain, and so that, so that all of our members can learn from it.

Dugan Petty: 31:16
And if we see a vulnerability and observe something out there, uh that we, that that people, have the opportunity of taking action, as opposed to it happening in a state and and they don't, and they don't talk to anybody about it, nobody knows about it. Well, if we begin to make those kinds of things more transparent, then we can say, well, wait a minute, that could happen here. Maybe we should do this to solve it, or you know that happened here and this is what we did to solve it and share that solution. So those are really appropriate, good next steps, it seems to me, to help us all get stronger in this area together.

Josh Descoteaux: 31:56
Dan Russ, what do you envision the relationship between NCSC, NASPO and everybody that has a vested interest, which is pretty much all of us? How? Do you see this relationship playing out and what are some next steps?

Russell Porter: 32:10
There is.

Russell Porter: 32:11
Well, I think Dugan hit the nail squarely on the head.

Russell Porter: 32:16
I would just add to it by saying you know, organizations like the National Counterintelligence and Security Center are not large, there's not a huge staff, and so we rely on associations like NASPO in order for us to ensure that procurement professionals across the country are getting the kind of insights and information they need and to convey it in a way that it makes sense to them.

Russell Porter: 32:44
And so, in that sense, naspo is not only helps us with that one-to-many relationship that we have to have, but also is a translator for us. So we have a lot of resources that are posted on our public-facing website, ncscgov. On our public facing website, uh, ncscgov uh, a ton of references and resources. But, as Dugan said, um, we have people who are engaged in a bunch of um meetings and and fora that um to which many others don't have access, and so, uh, having that relationship, uh is is really vital in order for us to carry out our mission. And I'll just close by saying, you know, we have to have it as a true partnership. Often, people or organizations do things at one another or to one another in some cases and we really want to make sure we're partnered with.

Kevin Minor: 33:41
ASPO. I think that's a good distinction.

Russell Porter: 33:43
To make sure we've got the procurement professionals taken care of in this area.

Kevin Minor: 33:48
I think that's a good distinction to make. I really do so before we go, and we'll make sure, Russ, we'll make sure that

we put a link to that resource that you mentioned. We'll make sure that we put that in the show notes for this episode so that it's easily accessible. Sure that we put that in the show notes for this episode so that it's easily accessible. So, before we go, one thing that we like to do is we like to ask our guests what's some advice that they have for our listeners. This advice can be professional Obviously you've shared quite a bit of wisdom with us today but it also can just be you know, don't eat yellow snow, right? So, before we go, what's some advice that you would give our listeners, Russ the?

Russell Porter: 34:29
advice I'd give everyone is as much as we've talked today about how gloom and doom it may sound, it doesn't have to be gloom and doom. There's something everybody can do to help make sure the world's a safer, better place. And take those steps. Don't just think about it and do them.

Kevin Minor: 34:49
That's a good one. Don't think, just do or think and do. Right, dugan, what about you Do?

Dugan Petty: 34:59
you have any advice for our listeners? Take your CISO to lunch, if you're a chief officer, and have a. Have a conversation about third party risk management and what a good next step might be, or if you need it at all.

Kevin Minor: 35:15
That's great, absolutely, absolutely. Russ Porter is a senior executive at the National Counterintelligence and Security Center and Dugan Petty is a cooperative contract coordinator for NASPO ValuePoint Gentlemen, thank you guys so much for talking with us today. We really appreciate it.

Dugan Petty: 35:36
Take care. Thanks, Kevin.

Russell Porter: 35:38
Kevin Josh. Thank you and thanks Dugan Russ. Great talking to you again. Great talking with you. Thanks, dugan.

Kevin Minor: 35:44
Man. Isn't it just a treat, josh, thank you. And thanks to Russ. Great talking to you. Again, great talking with you. Thanks to man. Isn't it just a treat? Like I could listen to those guys talk all day long. And, like Russ said, I don't think it has to be all doom and gloom, right? I mean, there are ways that we can educate and mitigate these risks, things both that we're already aware of and some that we may not be. These risks things both that we're already aware of and some that we may not be. Regardless, we will be here for you to continue to bring that information, to keep bringing you that conversation that you may need to hear. I know you want to hear it. That will do it for us on the Pulse today. Again, if you haven't already, make sure you subscribe to us on Apple Podcast, podcast, spotify, google, and make sure you check out the NASPO blog that is pulsenaspoorg and catch up on those articles written by your very own NASPO staff. I'm Kevin Miner. Until next time, bye.