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.

Amanda Valdivieso: 0:12
And I'm Amanda Valdivieso.

Kevin Minor: 0:14
It is technically your third Pulse podcast. I say technically, because I think we had that one special episode.

Amanda Valdivieso: 0:20
We did with Bart.

Kevin Minor: 0:22
Yeah, yeah, and we'll count that, but we don't count that. So this is technically your third Pulse podcast. What do you think? So far are you having a good time.

Amanda Valdivieso: 0:30
I'm having a great time, kevin. It's been a lot of fun getting to talk with all of our different um guests and just getting to be with you. Every uh episode has been a blast oh, I'm blushing. I know it's because we have so much in common. I just just love talking about all of our nerdy stuff together.

Kevin Minor: 0:48
We do. We do we always warm up before we start these recordings and we'll talk about what we liked and disliked about the latest comic book or movie fad. We do.

Amanda Valdivieso: 0:58
It is a lot of fun Beacon of nerdy stuff. So today we're going to be talking about cybersecurity, right? Not that it's nerdy, but I mean I think it's pretty nerdy but it's definitely nerdy in a good way. It really is, and it's been such a hot topic lately. You know, I know, recently there was a major breach with Facebook. This, the breaches that are happening, the record breaches are just coming at an astounding rate. You know, in 2016, about 95 percent of breach records came from only three industries, and that was government retail and technology.

Amanda Valdivieso: 1:27
A lot of our listeners work for the government right, I think. During the pandemic the FBI did report like a 300% increase in cyber crimes because everyone was moving from the office to the home space, where they might not have the same cybersecurity protocols as their workspace did.

Kevin Minor: 1:47
Right. Well, luckily for our membership and for those in government and those other agencies that you mentioned, there are a lot of different organizations that are taking charge and trying to mitigate some of these cybersecurity risks.

Amanda Valdivieso: 2:04
Exactly, yeah, one of those is StateRamp, correct.

Kevin Minor: 2:07
That is. That is and that's why today on the Pulse, we are talking with Leah McGrath, who is the executive director for StateRamp.

Amanda Valdivieso: 2:14
And what exactly is StateRamp Kevin?

Kevin Minor: 2:16
Well, we're going to find out. Amanda, you got questions, comments. We'd love to hear from you. Email us podcast at naspoorg and, if you haven't already, make sure you subscribe to us on Apple Podcasts, spotify, google or wherever you get them. Sweet listenings. Make sure you check out the NASPO blog, pulsenaspoorg. Let's take the pulse, leah. Thank you so much for joining us today. How are you?

Leah McGrath: 2:42
I'm great. Thank you so much for having me.

Kevin Minor: 2:45
Thank you so much for taking the time to talk to us today. How are you? I'm great. Thank you so much for having me. Thank you so much for taking the time to talk to us today. You are the executive director of StateRamp. I know basically that StateRamp is a platform that helps states to verify whether cloud service providers, that's, csps, meet a state's published cybersecurity policies. We're going to talk a little bit more about what StateRamp is in a minute, but first can you describe your responsibilities as the executive director?

Leah McGrath: 3:14
So I was appointed to be the executive director by our StateRamp steering committee in the fall of 2020. And as the executive director, I have had the privilege and opportunity to work alongside the steering committee for over a year, really developing and dreaming about what was possible and now, in 2021, launching the State Ramp organization, and so my responsibilities include a lot of outreach and awareness activities, working with our governance committees, our board of directors and standing committees, and then helping develop and refine our processes to make sure we are best serving all of the stakeholders.

Kevin Minor: 3:55
And what does that outreach look like? How's that been going?

Leah McGrath: 4:00
It has been an exciting first quarter of 2021. Our primary focus in 2021 has been purely outreach and awareness and making connections with state and local government officials, with the service providers and with the third-party assessing organizations, those independent auditors who do the audits and assessments to verify security. So in the first two months of 2021, we've spoken to over a thousand people. We're right at about 1,200 who have attended briefings and webinars and are really focusing now on kind of these special briefings for trade associations and organizations to try to reach and meet the stakeholders where they are. So the reception has been very positive every day.

Leah McGrath: 4:55
I receive an email from someone who says how do I join and how do I get involved, and so we are really excited about the momentum and really the groundswell of support.

Kevin Minor: 5:05
Yeah, yeah, that was going to be my next question is just how has it been received?

Leah McGrath: 5:19
But I'm not surprised to hear that there's been a void in how to efficiently and effectively manage and verify cloud security, but not just for state and local government officials. That gap everyone was aware of. I think the gap that maybe has been more realized in the last few months as we've launched this initiative, is that service providers feel

this as well, and so having to have these one-off procurement requirements, these verification processes that can just differ slightly from state to state or local government to local government or procurement to procurement, is really costly in time and also just costly in process. So the ability to have this kind of centralized process for verification where you can verify and use once has been really appealing to the provider community as well.

Kevin Minor: 6:15
Yeah, absolutely. How did you come to understand the importance of cybersecurity for state and local government?

Leah McGrath: 6:26
cybersecurity for state and local government.

Leah McGrath: 6:27
I'll talk more personally for a moment and I can talk about how StateRamp came to be realizing that need.

Leah McGrath: 6:32
But my background is in government policy and administration and have had a chance throughout my career to work within state government, but also served as deputy mayor for my city for five years and as we were modernizing and really shifting more to digital government services, the challenge is how to do that in a smart and safe way.

Leah McGrath: 6:58
As stewards of the government data, as stewards of the people's data, there's a responsibility to take care of that and to protect it. And so, as we were, you know, a part of that modernization effort. I really came to understand, in working with our IT director and our chief information security officer, the challenges inherent to that, and so, on a personal level, through the modernization efforts, it came to understand just how challenging that is, and you know citizens expect the same kind of services from state and local government that they receive at, you know, amazoncom, and so they expect and they want the you know kind of speed of business, if you will, within government services, and governments often asked to do more with less, and I think that's true across the board, and so realizing this was a challenge and a need. Although every state and local government is organized slightly differently, it's a very common need.

Leah McGrath: 8:06
Right you know, so imagine that's how StateRamp came to be is there were conversations at NASPO, there were conversations at NASIO, there were conversations in different states, and right. And with providers saying there has to be a better way.

Kevin Minor: 8:21
Yeah.

Leah McGrath: 8:22
And in 2020, at the start of the pandemic a steering committee actually was forming and started asking that question what if? What if we could come together to create a common set of recognized standards, a common method for verifying these standards? What difference could that make in helping raise the posture, the cybersecurity posture for everyone?

Kevin Minor: 8:48
Yeah, yeah, and it's such an ever changing environment too, right. I mean there's always new threats in the cyber space, right In the cyber realm.

Leah McGrath: 8:59
Every day. You can't go a day and I you know. Now I have my Google alert set, so I receive every single day and read about them.

Amanda Valdivieso: 9:07
There's a breach or a threat and it's absolutely the greatest risk probably that our country faces Terrifying it is, you see it, at corporate America level, so you can't imagine it's not happening at our state and local government.

Leah McGrath: 9:21
Well, and state and local. There's a lot of data on that, and state and local governments are very often a target, because there, you know, is a perception that maybe they haven't been as secure, and so they're a common target, they're a common victim. I think it's underreported and it's absolutely a need. And I will say with you know, the end of 2020, when we saw what happened with solar winds really got a lot of attention, but not just that, I would say 2020, we saw a massive shift, out of necessity, because of the pandemic, to move more to digital services and a digital environment, and so this the timing. You know, I was talking to JR Sloan and he is the president of the board of directors and he is the chief information officer for the state of Arizona, and we were talking about this and he said I think this is the right solution at the right time, and I think that's why you're seeing, you know, kind of that's wonderful, so much interest yeah.

Amanda Valdivieso: 10:24
So Leo just sitting, that's wonderful, so much interest. Yeah, so Leo just sitting here thinking about it. So we've kind of given a broad overview of StateRamp and you've talked a little bit about the vision, the vision of this common standards, common policies coming together. Let's talk about StateRamp as a whole a little bit more in detail. The meat potatoes, what is it?

Leah McGrath: 10:39
doing Absolutely so. I mentioned that steering committee, and you can view who the steering committee members are if you go to stateramporg slash leadership. But they are dozens of state CIOs, chief procurement officers, chief security officers, private industry, subject matter experts. We've got former state CIOs, CISOs involved, and it is just a collection of really smart, thoughtful people that I am privileged to have worked with. Who came around that question of what? If? So, if we did try to bring people together, what would it look like? How would it be governed? How would it be funded? Yep, who would define the security requirements in that process? And so what they've come to and you can see all of this documented at stateramporg slash documents but is StateRamp has formed as a nonprofit organization we're organizing as a 501c6, which is a membership organization, and our focus is really bringing states and local governments together with the providers who serve them, to educate on best practices, to identify these standards which you know you mentioned.

Leah McGrath: 11:59
They change, they do right. It requires that ongoing vigilance and so, bringing everyone together, we have a board of directors that is comprised of a majority of state and local government officials. There is minority representation for private industry and subject matter experts, and so then we've got standing committees as well who advise on those standards and technical matters. We have an appeals committee, so if there are questions or deviations, those can be settled by the appeals committee and then we have. So the steering committee spent a lot of time evaluating standards and what we found in talking with most states if not all have adopted a cybersecurity framework based on NIST. Those are the National Institute of Standards and Technology widely accepted standards in cloud security and so it's based on NIST and that's something that we'll be keeping an eye on, of course, and educating on Is that public and private both have adopted NIST.

Leah McGrath: 13:18
Yes, it's widely accepted. Okay, yes, yes.

Kevin Minor: 13:21
Cool Interesting.

Leah McGrath: 13:23
Yeah, so widely accepted standards that are also required. It's the backbone of FedR. Can't? States and local governments just rely on FedRAMP? Right, and we know some do To be FedRAMP authorized? Fedramp is a federally funded office within the GSA that is responsible for verifying the cloud security of service providers, and in order to do business with the federal government, the providers who wish to do business with the federal government must be FedRAMP authorized. To be FedRAMP authorized, you must maintain a minimum contract with a federal agency.

Amanda Valdivieso: 14:19
Okay, the caveat that's the caveat.

Leah McGrath: 14:22
There are a couple caveats. One is that so if you're interested in leveraging that as a state or local government, you would be excluding the vast majority of providers who you may be working with the smaller and the medium providers who don't do business in the federal government. So FedRAMP doesn't work for those providers. But also, what we've heard from state and local government officials is it doesn't always work for them either, because they don't have access to the documentation. They're not receiving notifications, right. So it's hey, I have to go to a website and just look and take the word for it. So that is why FedRAMP doesn't work for state and local governments. But they do have a process identified that relies on third-party assessments. So StateRAMP is based on NIST and modeled in part after FedRAMP, and the idea with it is that a state or local government would adopt a policy Most of them have these policies in place already that require the vendors with whom they work to comply with their cybersecurity standards.

Leah McGrath: 15:30
So most have that already. Of course, the difference here is you verify it. It's trust but verify. So you adopt a policy that says, hey, you have to meet our standards, but you also have to verify that you meet our standards via independent third-party audit using StateRamp. So then the providers who wish to do business with that state or local government would need to engage a third-party assessing organization to do that independent audit.

Leah McGrath: 15:57
The audit is provided to StateRamp and we manage the PMO who receives that information, who verifies it and then who also has responsibility for that continuous monitoring activity. And that's the real difference maker, I think, when you talk to states and local governments is you know audits can be, you know you can have an audit or you could, you can do kind of one look and that's a one moment in time. But we know cybersecurity it's really about if we're going to get, if we're going to lift all boats and be better. It's about shifting the mindset to one and that culture to be one of continuous improvement, and so that's how this is modeled and that's how the process works.

Leah McGrath: 16:42
There are different impact levels. So you know, depending on the criticality of the system or the sensitivity of the data, and so that's how this works and how it's funded. I think one of you had mentioned that earlier. How is this funded? It's a membership organization, so states and local governments can become a member at no cost, but the Wait.

Kevin Minor: 17:09
I don't think the folks in the back heard that yes. Can you say that one more time.

Leah McGrath: 17:14

So there's no cost for states and local government officials to participate. If a state or local government wanted to adopt StateRAMP, we have kind of a letter of agreement or a membership agreement that then they can note and this can be at the agency level. We have several states who are looking at this at the agency level.

Leah McGrath: 17:33
So, an agency could say here's my primary point of contact and if we know who that is, then they can be given an account within a secure system to be able to have a dashboard view of all the providers with whom they're working. So they get that monthly update, they can see what's happening. If there's an issue, they can be notified immediately. So it's that kind of trusted source of information.

Kevin Minor: 18:00
With staff right To back it up. Yeah, Actual staff Right and it works because we're really leveraging a shared service in doing it.

Leah McGrath: 18:11
So the providers are verifying one time and the PMO is receiving that information one time but able to share it out right to all of the states or local governments who've been contracted with that provider. And so that's how we are really maximizing our resources, by working together, I would agree.

Leah McGrath: 18:33
Yeah, so the providers. There's a membership level for service providers and that's called a subscriber membership. There is a fee it's $500 per organization this year to join and by joining the state ramp, the subscriber members or providers have access to education and resources and the templates and the ability then to list their product on the authorized vendor list. Now to be listed, you have to comply with all the security requirements we talked about and have that third party independent audit and then that's how they're able to be listed and then to maintain that listing, continuous monitoring requirements must be met.

Leah McGrath: 19:19
What do you look for in a provider? I'm looking for any. You know we've had over 800 providers participate in calls in the first two months and I've had several one-on-one calls and I've had these one-on-one calls with large providers, small providers.

Leah McGrath: 19:43
You know our mission is education. We want to see these providers succeed, so we've really tried to strike that balance between business friendly and maintaining the integrity of the verification and maintaining the integrity of the verification. And so you know what we're looking for are providers who want to do business with state and local government, who value cybersecurity. Inherent on cloud service providers these days is to ensure and validate that your systems are secure, and you know we're all in this together. So you know any provider who's interested, whatever the maturity of the cybersecurity model that they have. We want to be able to help meet them where they are and take them through this process.

Kevin Minor: 20:45
Well, so it sounds like you know the representation and just how the organization is set up is very thoughtful and I appreciate that.

Leah McGrath: 21:03
I feel like you've really done your due diligence in setting this up and everyone's represented and you've really covered all your bases.

Leah McGrath: 21:06

Well, thank you, and I want to make sure that you know that is not because of anything I did. I had the opportunity to work with some really thoughtful individuals. You know we have our board of directors. We have a small board who leans on our steering committee. So our board, with JR Sloan, who's the chief information officer for the state of Arizona, Ted Cotterill, who is the chief privacy officer for the state of Indiana, expertise and resources to help get this started. But then you look at the steering committee and Terry Takai. She's got just a great resume of experience with state governments and with federal and working now across so many organizations to help improve cybersecurity and processes. So the list goes on and on, but Dugan Petty.

Kevin Minor: 22:02
We've got some NASPO members we do.

Leah McGrath: 22:03
I was just going to say We've got some NASPO members in there Dugan Petty from NASPO Value Point, jamie Shore from Maine, steve Nettles from Arizona.

Kevin Minor: 22:11
We're never above a shameless NASPO member. There you go.

Leah McGrath: 22:13
I mean On the pulse, above a shameless NASPO message. There you go. I mean On the pulse.

Kevin Minor: 22:16
So what is the role that State Ramp plays in educating state officials about cybersecurity? What is that relationship for procurement?

Leah McGrath: 22:27
That's a great question. So one of the things we heard early on in our steering committee meetings when we first started meeting to ask this question of what if Now, remember, we have members who represent procurement, we have members from our information security officers, and so you know, there were a few meetings where, you know, I joked that StateRamp was the bridge between and it became a little bit. I agree with that and it became a little bit. You know, you had information security officers who were recognizing the challenges in managing third party risk. But cloud security and cybersecurity, it moves very quickly and so how to kind of manage that third-party risk can be a really big challenge alone.

Leah McGrath: 23:21
But then you think about really where the rubber meets the road is in procurement. So how do you set these standards and make them flexible to meet the latest need of the day, and then how do you implement them from a procurement standpoint? And there was just this gap. And so StateRamp, I think, helps bridge that and I think, the way that you'll see it, progress as we continue to educate on these standards. It's bringing people together. It's bringing people together to say do we all agree on these standards and where are the commonalities, that we can leverage the shared service and then continue to educate on it.

Leah McGrath: 24:02
And so, whether that's webinars, we have, you can see just ongoing events that we have at staterampорg slash events. So that's a great opportunity and we're always willing to hop on a call or have a meeting to do. We've been doing a series of just agency briefings. So, as states are saying, let me pull a group of people together who are stakeholders or we've talked to some counties as well so that we can do this really direct agency briefing that allows for more Q&A to think about what does it mean for their state?

Leah McGrath: 24:38

And you know, one of the things that we've talked a lot about and I think is important to convey is that all procurement decisions always stay with the state. Right, like the state. Those decisions will always stay with the state. What StateRamp can do is bring people together to recognize common standards, best practices and then give visibility. Through that authorized vendor list, we'll give you visibility, or through that direct portal with your point of contact, you can have visibility into the risk postures of the providers with whom you're working so that you can make, as a state, risk-based decisions, so that you can standardize your procurement process in a way that is fair to all, easier to implement, reduce friction of these one-off procurements that we hear about, and make risk-based decisions that are right for you, and I think that's the flexibility.

Amanda Valdivieso: 25:40
So, leah, tell us how exactly does a state participate in this project?

Leah McGrath: 25:45
Absolutely so. There are a couple of opportunities for officials or employees who are of a state or local government to participate. We have memberships at the individual level. Go to stateramporg email info at stateramporg and we'll definitely connect you and make sure we have your information if you're interested. And those are really for individuals with responsibility for procurement or information security or privacy.

Leah McGrath: 26:14
In terms of how a state participates, if a state is interested in adopting StateRamp and when I say that I mean requiring third-party assessments and you know, kind of becoming a part of StateRamp then we have a letter of agreement that we can work with the state to execute. That we can work with the state to execute and it's different with every state. At some places that can be executed by the chief information officer and others you might want to have the chief information officer and procurement officer involved, but really what that does is it just becomes this letter of agreement between StateRamp and the state so that you know what the deliverables are for StateRamp and StateRamp you can name who's our point of contact. And, like I said, some states are doing this at the agency level. So we could have an agreement with each agency so that whomever is responsible for that third-party risk management. We can have that contact, give them an account within our secure portal so that that and in many cases it's the CISO or chief technology officer, whomever is assigned for that agency to manage that third-party risk and so then that person has a secure account where, once they're in, it's really assigning views so they can have a dashboard view of all of the providers with whom they're working, so they can see kind of the high-level summary of continuous monitoring, reporting, monitoring, reporting, see what's happening, month to month updates to their security systems.

Leah McGrath: 28:03
But then also, if there is a breach, if there is an issue, if there is a significant change, the PMO will notify. Then that primary point of contact for the state or for the agency so that you can stay on top of knowing what the risk postures are and that's really what this is about is just awareness and visibility. And so you know, we've talked to a lot of states and we've talked to a lot of states who have gone through the process of vendor verification. Yeah, but the piece that most states I haven't talked to a state yet who has the budget or bandwidth to do or maintain is that continuous monitoring. So, and we know, in cybersecurity and cloud security. That's probably the most important part. It is, you know, it's not just getting your policies in place, but it's also making sure that you're staying on top of it, month after month, and as you're adding new features, as you're adding new plugins, that you're continuing those good practices, and so the continuous monitoring for the information security officers is really that difference maker.

Amanda Valdivieso: 29:12
I would agree with that. I think that trust but verify the continuous monitoring is such a huge aspect of.

Leah McGrath: 29:18

StateRamp.

Amanda Valdivieso: 29:19
So if states are interested in adopting StateRamp, what do they have to do now to start preparing?

Leah McGrath: 29:25
Absolutely. We have a getting started guide for government that you can find if you go to stateramporg slash documents. You can also email. You could email me or you can email info at stateramporg and request a meeting and we are happy to hop on the call and walk through that getting started guide. But it really starts with adopting that policy. That requires the independent verification, that trust, but verify your cyber policies. It's that letter of agreement with State Ramp so we know who is the contact so that you can have access to that information and then you know we'll be rolling out here in the next few months sample policies, sample standards, sample procurement, language the other states are working on, so they're doing the work on our behalf so that we can we can just share that with everyone. Yeah, that's wonderful.

Amanda Valdivieso: 30:20
Yeah, yeah, I think those samples will help a lot of people. I do too.

Kevin Minor: 30:24
Yes, You've dropped a lot of really important links and we'll make sure that we put all those links in the description of this and make sure that we, that our membership is connected, our listeners can connect with you Exactly.

Leah McGrath: 30:36
Awesome, thank you.

Amanda Valdivieso: 30:38
So, Leah, before we go, do you have any advice for our listeners in regards to StateRamp cybersecurity? Do you have anything for our listeners or general life advice? Life advice with Leah.

Leah McGrath: 30:48
I don't know, I'll stay away from that one Okay.

Leah McGrath: 30:54
You know. No, I am really encouraged by the um reception that we've had and the questions. I love when we get on a phone call with some individuals who are skeptical and have, you know, 20 questions because I learned from that call. Our team learns from that call as much as um I think the uh person on the other line does and so you know. It's about recognizing the need for third-party risk management. It's about recognizing that there's you're not alone, that you know every Nice to realize that it is Every state and local government is dealing with this for sure.

Amanda Valdivieso: 31:36
You know every Nice to realize that it is Every state and local government is dealing with this for sure.

Leah McGrath: 31:39
You know, and you know, I've had one-on-one phone calls now with 25 states, and I can tell you every state is facing this in some way and trying to figure out the best way to deal with this. I think there's. You know, our procurement officials, our chief information officers and security officers, technology officers, privacy officers they are really feeling the weight of responsibility to be good stewards of our data and of our systems and to protect our infrastructure from cyber attacks, and so I think that the desire is there, the shared need is there, and, just if you have questions, I encourage you to get involved and ask. Because you mentioned this, I've said it, we're at 1.0. And

a lot of thoughtful work has gone into getting us to this point, but we know that there's a lot of opportunity for growth in the future too, so encourage you to get involved.

Kevin Minor: 32:46
Sounds like the sky's, the cloud's the limit right the cloud's the limit and we've talked about.

Leah McGrath: 32:53
You know, every call I get on you start hearing some common themes and we've had this in our steering committee to say you know what about CJIS and what about IRS requirements and what about Marcy 2.0? And you know we're starting with cloud security. That's where we had the most common shared set of standards. To start with, most have adopted a cybersecurity framework based on NIST, but I do think there's opportunity moving forward. You know, if we can get this model right, there's opportunity to bring everyone together for these other common sets of requirements too.

Leah McGrath: 33:28
And so you know, when you look at the horizon and what's ahead, it's really exciting.

Kevin Minor: 33:34
That sounds really exciting. That sounds really exciting and my hope is that we can have you back on the pod in a year and we can see we can talk about.

Amanda Valdivieso: 33:42
Yes.

Kevin Minor: 33:43
What the next adventure is it would be fun. Leah McGrath, executive Director, state Ramp, it was a pleasure to speak with you today. Thank you so much.

Amanda Valdivieso: 33:54
Thank you. So it sounds like they really got their act together.

Kevin Minor: 33:57
It really does. I'm excited to hear our future follow-up episode with her.

Amanda Valdivieso: 34:02
Me too. Like she said, it's still on version number one, but it really sounds like they've really put some thought into connecting the dots and keeping up with the ever-changing cyber realm, like you were saying.

Kevin Minor: 34:13
Ooh, cyber realm yeah, I like that. That sounds like a cool place. I'd like to go sometimes, but it's also a scary place.

Amanda Valdivieso: 34:20
Yes.

Kevin Minor: 34:21
And we need to keep that in mind. We also need to tell the members where they can go to connect with Leah so that they stay protected.

Amanda Valdivieso: 34:28
Yeah, kevin, exactly. You can find their getting started guide for the government that she was talking about by

going to stateramporg slash documents. You can email them at info at stateramporg slash documents. You can email them at info at stateramporg. And in the interview she encourages states to request a meeting. They'll actually walk you through how to get started and you can also find all of that information out in the description of this podcast as well.

Kevin Minor: 34:52
Also also it's free. It is free, free, free, free, free, free, free, free, free, free no money down, no money ever no money up there, no money around here, no money free, free, free all day long. Thank you,