Telice Gillom: 0:03

Welcome to another episode of the NASPO Pulse podcast, your go-to source for state procurement chat. I'm your host, Telice Gillom, and for today's episode I've got my fabulous co-host joining me once again, the illustrious Megan Smyth, NASPO's Director of Legal Education. Megan, thank you again for joining me for this conversation.

Megan Smyth: 0:25

Well, thank you for inviting me back, Telice, and I think you're setting everyone's expectations really high by using words like fabulous and illustrious, but I will try to live up to that.

Telice Gillom: 0:36

Of course you can.

Megan Smyth: 0:38

So today we're going to be discussing the most difficult terms and conditions that we encounter in state contracting, what we should know about them and how to negotiate the best terms for the state. I strongly encourage everyone to follow up on everything we say with your own internal counsel. This is not legal advice. Nothing I say here will be upheld in a court of law if you rely on this, but we are providing very general information about the generalities of these terms and conditions. Your state law may be very specific on some of these requirements and some of these things may not be allowable in your jurisdiction, and some of these things may not be allowable in your jurisdiction. So please speak with your attorney before you take any of the advice we give you here to heart and use it in practice.

Telice Gillom: 1:32

We're discussing these terms and conditions because these are some common challenges that come up in procurement offices between legal and procurement staff.

Megan Smyth: 1:40

Absolutely, and we want to provide some general insight into what these contract clauses mean and explain how they can affect the agency from both a legal and a procurement perspective.

Telice Gillom: 1:51

Now remember you should subscribe to the NASPO Pulse podcast so that you never miss an episode and always feel free to email us with your questions.

Megan Smyth: 1:59

Telice let's take the pulse.

Telice Gillom: 2:01

We are back with our second installment of Terms and Conditions for Procurement, and, megan, I am excited. What about you?

Megan Smyth: 2:12

I'm pretty excited, you know. I know that our listeners probably have other podcasts in rotation. They listen to True Crime maybe. Maybe they listen to you, listen to NPR news podcasts, but this, this conversation, will be the most tantalizing thing you hear today.

Telice Gillom: 2:33

I don't think there's anything else more exciting than this. Picture your favorite music legend performing a concert just for you.

Megan Smyth: 2:43

In your backyard.

Telice Gillom: 2:44

Just for you, not as exciting as terms and conditions.

Megan Smyth: 2:50

No, you will not learn as much. I guarantee you that you would not learn as much. That's true, that's very true. You're going to learn something today.

Telice Gillom: 2:59

That's true.

Megan Smyth: 2:59

Cyber liability, insurance Three exciting words. All attorneys get excited when they hear the words cyber liability and insurance all in the same phrase.

Telice Gillom: 3:09

I think they probably click their heels together. They just can't contain their excitement.

Megan Smyth: 3:14

Jazz hands are maybe happening.

Telice Gillom: 3:17

I do jazz hands all the time. It's exciting stuff.

Megan Smyth: 3:22

Tell us all about it. Well, speaking of stuff, we don't want people touching our stuff.

Megan Smyth: 3:27

That's right, that is the theme of today's contractual terms. So a lot of this we're going to be talking about protection. This is protection of the state's assets, the state's data, the state's intellectual property, etc. Etc. So this is a very defensive sort of set of terms, but that's a good thing, because you got to have a good defense and a good offense in a contractual situation.

So let's start with cyber liability insurance and see where this exciting journey takes us. What do you say? I'm with it, Okay.

Megan Smyth: 4:04

So what is cyber liability insurance? It protects the state from financial losses that are related to data breaches, cyber attacks and other digital risks. And if you're asking yourself, well, what expenses could there be? Because it's all unfortunate when our data gets breached and we usually see it on the news and it's usually some giant company that has all their customer data has been released to the public. And what we're concerned about in that situation is personal identifying information, or PII, which is information that will tell you who a person is. So birth date, social security number, address, email address, Sometimes it's just a combination of those things. So a lot of people think it's fairly innocuous to give out your email address or your home address, but, combined, all that information can in fact, be dangerous.

Megan Smyth: 5:04

Coverage for cyber liability insurance can include a lot of things and you can get basically bespoke coverage if you pick and choose which elements of the coverage you want. So that can include data breach, response costs, the legal expenses, regulatory fines and penalties, business interruption losses, cyber extortion payments I mean, come on, that is exciting. That's some true crime right there or reputational damage mitigation. So cyber extortion is actually a pretty sexy topic, if we want to say anything in this area. It's sexy right now and it is the talk of the town and a lot of people will hear this as ransomware or ransom attacks.

Megan Smyth: 5:48

Where the attacker. This happened in San Francisco many years ago. The public transit system was held hostage and it's basically, if you don't pay me, no one will be able to ride the Metro today, which you can imagine in a big city like San Francisco the kind of disruption that would cause. So that's basically holding the data hostage or holding a company's whole system, enterprise system, hostage until they pay a certain amount. And in order to know what you need, what kind of coverage you need, it is important to do a very thorough risk assessment for each procurement and determine whether cyber liability insurance is something you should consider.

Telice Gillom: 6:33

This is the type of thing that the procurement officer should be looking at before the solicitation goes out.

Telice Gillom: 6:41

Indeed, at the beginning of the process, as soon as you're talking with your end user department or your end user agency about your specifications for the IT product or service, the risk assessment for your cyber liability insurance should be included in that conversation, because whatever that risk assessment is going to look like, the parameters of that should be included in your solicitation, and you should make it very clear at that point what you'll need to say and how you'll need to say it.

Telice Gillom: 7:15

Again, chum up with your legal staff, because they can help you and guide you to what it needs to say to make sure that you're really covering the agency's best interest in the solicitation. So you said it right out front hey, supplier community, this is what we need from you in the way of cyber liability insurance, so that there's no question on the other end as far as what you need and they're not giving you less than what you need. On the back end, there's no room for negotiation. When you get to the negotiation stage, they're not saying, well, here's less than what you told us you needed. We know that. You said you needed a million dollars worth of coverage, but we're offering you a hundred dollars worth of coverage. Can you accept that? Because then you can say absolutely not get out of our faces right and during before you write the solicitation.

Megan Smyth: 8:19

If you're doing a q a, for example, it's a good moment to say this is what we think the cyber liability is for this contract. If you disagree, we would love to see your risk assessment. Why you think it's less and you know no reasonable state is going to be like. No, I don't even want to hear that. Like you, at least want to know what's going on out in the marketplace, especially so if you have certain requirements in your solicitation for, let's say, pandemic coverage, which maybe doesn't exist right now because we just went through one. That's a problem that needs to be addressed up front, and you're probably going to upset your suppliers and break good faith with them if you aren't honest with them up front, because they're going to put time into that bid and if it turns out in the end they have to have a million dollars of cyber insurance they're never going to qualify for Right. What was the point of all of that? And so it's important to know specifically whether this contract is going to require the supplier to carry coverage, or the state is going to carry coverage, or you're both going to carry coverage, in which instance you would want to talk about which coverage is primary, so which coverage goes first in the stack of insurance policies that you may have in any given situation and typically and that can be difficult when dealing with suppliers If you're asking them to take on all of the risk for a contract, that's not fair and you're not going to get any quality bidders at that point when you're asking them to take on all of the risk discussed.

Megan Smyth: 10:11

The tech landscape is quite mercurial and if you wrote a cyber coverage policy in January of 2020, I guarantee you that by today and not just because of the pandemic, because of think about how far AI has come in the last four years you may be lacking in the availability of remedies, in knowledge of the actual threats that are out there, and your coverage may not be good after even six months.

Megan Smyth: 10:34

So a re-evaluation process is very important as you move forward. Premiums can be really high for this coverage, especially right now when people are kind of in a little bit of a panic mode about it, especially if you add in ransom coverage, and there is a report that we'll talk about when we get to data protection from IBM, and they do a great job of explaining the cost

related to a data breach in a myriad of different circumstances and industries, and so I highly recommend people take a glance at that report, you know, look at it when you're doing your risk assessment, maybe use it to help you evaluate the solicitation you're working on and you want to make sure that you're updating when you do that evaluation. You need to update the policy to talk about current risks and threats, um, and you want to be sure that you have the right kind of coverage. So if you don't understand the policy when you read it, find somebody who does to go talk to your attorneys. Um, insurance contracts can sometimes be purposefully confusing.

Telice Gillom: 11:48

Would they purposefully make them confusing?

Megan Smyth: 11:51

No, not confusing, and that's probably not fair. And I should be fair in this situation and say not confusing, but unclear, broad. You know we've all done it. You put a clause in a contract and it's very vague language and you do that because you think you may want to take advantage of that vague language. And you do that because you think you may want to take advantage of that vague language at some point down the road. So it's important to know what is vague and what is not.

Megan Smyth: 12:16

So, for example, if your coverage says we will provide you data breach response costs period, okie doke, what does that mean to you? What are you going to provide continuing credit coverage for the people who had their information put out? Are you talking about response costs with regard to getting the system back online, kicking the people out, rebooting the system, getting new security measures in place? What exactly do you mean when you say data breach response costs? And I would want a very clear explanation, definition of that that we all agree on and understand. All right, ready to talk about data protection and storage, which is also so exciting.

Telice Gillom: 13:05

Let's jump in with both feet.

Megan Smyth: 13:08

Okay, so I'm going to use the IBM report from 2023 for a lot of this conversation, because what it does is it provides a good, comprehensive, global picture. They use data from 533, 553 breaches even more in 16 different countries, and they take into account hundreds of cost factors. It's like a 60, 70-page report. It's very comprehensive. Again, if you're a nerd or particularly interested in cybersecurity or an attorney working on this Itime high, the average cost of a data breach in the US as of today is $4.45 million. That's a 2.3% increase from 2022, but it's a 15% increase from 2020.

Telice Gillom: 14:05

My eyebrows went up into my hair. That is huge.

Megan Smyth: 14:12

Wow, way past the rate of inflation, way past the rate of literally anything. So that's pretty crazy. And so again back to the point of making sure that your policy is up to date, that it is relevant, that it addresses current relevant dangers relevant that it addresses current relevant dangers. And they suggest primary areas for additional security investment. What they also do later in the report is they tell you what those, the post-breach, what the companies invested the most in, aka what they learned from their breach, and most often that is incident response planning and testing.

Megan Smyth: 14:54

So mocking a breach, mocking a ransomware incident and this is true in any kind of emergency response for a procurement office or any agency in the government really is.

Megan Smyth: 15:07

I, you know, I attended a conference shortly after some of the hurricanes happened in in the island nations in the caribbean and the puerto rico cio chief information officer was there and he was talking about how, when the storm hit, it was literally they lost everything.

Megan Smyth: 15:25

They lost power, they lost communications, they lost their cell phone, lost power, they lost communications, they lost their cell phone coverage, everything. And he said, if I had it to do over again, I would go back in my office on one random Tuesday. I would shut everything down. I would just turn all the lights off. I would turn all the computers off. I'd shut down the system and say, okay, let's procure some stuff and see what you can do. That's because you should mock the situation that you're going to be dealing with and so, in employee training and when training them on the things that we all know, you should train them on password protection, don't click on phishing emails, don't download unauthorized software, all those types of things. You also need to be talking about what to do when it happens, right, not if when Threat detection and response technologies can be expensive, but, man, they can save you on the back end.

Megan Smyth: 16:21

So, that's also something to think about investing in, and I'm sure that the reason that is a popular post-breach remedy is because you realize that if you had spent that money on the back end, you wouldn't be spending $4.45 million now to fix it, and I guarantee it's going to be less expensive on the prevention end than it is on the cleanup end, as it usually is. So using security AI and automation can reduce the costs and minimize the time that it takes you to identify and contain the breaches. So that can lead to a shorter time frame in identifying and containing the breach and can lower your data breach costs. So if you have extensive AI security you have automation to help you identify and contain breaches you could drop your cost from 4.45 to 1.76. That's a pretty big difference if you are using and these are all estimates, but if you're using appropriate security technology, that could be the difference.

Telice Gillom: 17:28

So we're talking about millions.

Megan Smyth: 17:30

The difference in millions of dollars, millions of dollars, yes, and we have the highest cost of data breaches in the world. The next closest to us, I think, is the Middle East, which they lump together for some reason as the Middle East, but they come in second. And then Canada is way, way below us in the 2 million range. So we are far above and beyond most of the rest of the world, but that's because we are a highly technologically dependent society at this point, and the public sector breaches are 2.6 million on average. So that's the difference between a public sector breach and a private sector breach, and so what our states are mostly dealing with are public sector breaches. But $2.6 million, I'm pretty sure I can think of some things the state could use that money for instead of dealing with a cyber breach, can't you? Definitely? Yeah, cool stuff like roads and schools and neat stuff like that.

Telice Gillom: 18:32

And we're talking about procurement. This is a part of the tenets of procurement is being good stewards of the public dollars. This is not being a good steward of $2.6 million.

Megan Smyth: 18:49

It's a lot of money, and 82% of the breaches in 2023 involved data stored in the cloud 82%. The cloud does not save you from anything, so do not think that the cloud is a magical, safe place to put all of your data. It absolutely is not.

Telice Gillom: 19:08

I think people thought it would be initially. Back when cloud storage was initially the new technology for storage, people thought, aha, now we will have this technology. So random maybe not random, but we will have this new technology that is more secure than saving things on a thumb drive, and this will save us from bad actors who seek to hack into our systems. Put as much stake in ensuring that their office staff were data literate with the cloud technology and something as simple as phishing emails.

Megan Smyth: 19:57

Yeah, and people would, I think, be surprised. You know, check the report out, because it lays out the source of the breaches and most of the time lays out the source of the breaches and most of the time it's internal, it's something they clicked on, it's a password breach. It's you're using the same password for everything. Yeah, it's unfortunate how much misinformation there is out there. I mean, I saw the other day there's a website where you can go and type in your password and it will tell you if it's safe or not. And I thought so. You're typing in your password to the Internet to ask if it's safe or not. It's just doesn't, doesn't seem like the right thing to do.

Megan Smyth: 20:44

So there's a lot of misinformation and I think people think, as long as they use the suggested, strongly suggested password from Apple or Google, that they're safe. You're not, and you

should train your staff attorneys alike to identify sketchy emails and to not open them and click on them. And I think the education piece is so important because you need to give them ownership over the situation, because otherwise it's just a government computer that you're using at work right, and maybe you're not going to be as careful as you would at home buying something from your private computer. But you should be. You should be as vigilant, if not more so, because you're dealing with the state's citizens' data. You don't want your data's in there too, right? Exactly.

Megan Smyth: 21:32

If you're a citizen of the state. Your stuff's in there too, so there needs to be a level of ownership and responsibility that they feel that they can help prevent this by following the rules and doing the things. And you know, IT officers are coming up with creative ways to do this. They send out test fake phishing emails to see how many people will click on it, just as an exercise, not to punish anybody, but to train people to actually pay attention to where the email is coming from.

Telice Gillom: 22:02

This is one of the things that I mentioned on the modernization webinar too. Mentioned on the modernization webinar, too, is that there should be a baseline of data literacy in the procurement offices, because these data breaches are very expensive, but also because it's not an option anymore. We talk a lot about technology myself in particular, because I'm a tech nerd what can I say? But as the procurement offices get more technical, just due to the times we live in, you can't go well. I don't want to do that that way. I don't want to deal with this digital process now. I still want to fax things or I still want to do the paper manual way of things. You don't have that option anymore and the policies, the procedures need to be updated to include these new technologies and everybody has to have kind of a baseline of knowledge of what the new technology looks like, how it affects you, what you should and shouldn't do. So that the data protection of everybody is your kind of knee-jerk reaction.

Telice Gillom: 23:33

It is your modus operandi. It's not just because you are in the procurement office and you have to be a good steward of the taxpayer money and it is ethical and et cetera, et cetera. It is how we used to have to get used to saying www dot and then we stopped saying www dot. Right, we moved on, we moved past that. Like time marches on, the lexicon marches on, and also your natural reaction to things also must evolve and march on, and this happens to be one of those things too. You know that you've got to evolve. You have to. You don't have $2.6 million to toss around. If you do call me, let's talk about it. Yeah, I know.

Megan Smyth: 24:33

But call us and we will take that problem right off your hand.

Telice Gillom: 24:38

I've got a school in my neighborhood that you could take that $2.6 million to.

Megan Smyth: 24:46

Yeah, yeah, I think we could all find better use for that money, and you know it's. It can seem a little intimidating, I think you know, oh, I'm just a contracting officer or I'm an attorney. I don't under, I don't, I went to law school so I didn't have to do math. I say that a lot, and it can be intimidating to think that you need to be an IT expert, exactly.

Telice Gillom: 25:08

On a geek squad or something.

Megan Smyth: 25:09

But that's not the case.

Megan Smyth: 25:11

In fact, the attorney ethical rules pretty clearly state that the point of being an attorney is learning to think like an attorney, and so you may not be presented always with the set of facts that you've seen before or a scenario that you understand completely, but you understand the law and how the law flies and how the law works, and so you take that knowledge and you apply it to this thing. So you may not know about cyber liability insurance, but you understand insurance, the basic principles of insurance, what we're doing here, and you build on that and you learn to get yourself to a level of competence where you can intelligently discuss it and the risks associated with it, and that's all. You don't have to write code or understand how it works, how the ransomware works. You don't have to understand that. You just need to understand what it is, what its purpose is and what risk it poses. That's really the main focus. So, as long as you understand to that level, you don't have to be an expert in IT to understand these things and contract for them.

Telice Gillom: 26:20

We're not asking you to turn into an IT wizard with your staff standing outside and your pointy hat saying you shall not pass to any cyber threats. You don't have to do that. I'll do that. I'll be there.

Megan Smyth: 26:37

Yeah, I wish we had that. I wish we had that. That would make it a lot easier. But yeah, no, and you know, look, I'm not pretending like this stuff is complicated. It is especially our next topic, intellectual property. You know patents, which is an area of intellectual property. There's a whole separate bar exam for that, like you take a whole other bar exam to learn how to be a patent attorney. Very, very complicated, but you can understand it. Enough to contracting the state government area with minimal effort. Staying up to date with the latest looking at our ProcurementU course offerings, listening to our podcasts and reading our blogs are a great way to stay abreast of what's happening.

Telice Gillom: 27:24

And that's why we're here. That's why we're here, right? If you have questions about these things, we want to know, we would love to help you understand. We know these things are complicated. That's why we're kind of talking about them in this lighthearted way with this series and with all of the podcasts and blogs, like she mentioned, is to explain this stuff in a way that helps break it down and make it relatable, and understandable.

Megan Smyth: 27:55

All right, let's talk about intellectual property. So when a state contracts for products or services, it is important to consider whether the state wants to retain ownership or usage for any of the resulting intellectual property. And what do we mean when we say intellectual property? It can be software, designs, reports or other creative works produced during the contract. So if you have contracted for creative services and they're creating logos and PowerPoint designs and marketing materials, stuff like that, you want to ensure that in the contract with that supplier, it is very clear who owns the finished product. When it's all said and done, who owns the actual thing that is created. And what that is talking about is key to answering the question right. Which thing are we talking about? Because we may or may not need it. What a clear intellectual property agreement will do is it will prevent you from having to repurchase things that the state has already paid someone to create, or do the cost of licensing something that you didn't get the rights to in the first place, or you can using continuing to use the products that the state has already paid for.

Megan Smyth: 29:29

So there is our specific laws, often regarding the use of IP created with public funds, and that's the key right. So think about it that way You're taking all the taxpayer money as a big conglomerate and you're using that to pay for this. So you're using public funds to pay for intellectual property. You want that to be available to the public. So proper IP clauses ensure compliance with those laws, and they often require that the work produced for state governments be accessible to the public. And when you make those clear, you're going to be able to protect sensitive information. For example, many IT contractors are very sensitive about their procedures and policies and how they do things. That's trade secret. We don't need that. We don't need to know that. We don't need to know how you did the thing, but we want the right to give that product to the public for their use and then ensure that the state can continue to use it into the future without bad repercussions.

Telice Gillom: 30:43

And this calls back to what we were talking about in the previous episode of terms and conditions. That would be a clear term and or condition or contract clause. We were talking about survivability. That's a piece of your survivability clause. Once the product an app, let's say is produced and it's working, it's great, we love it, the supplier has done their job and they've moved on. The contract in effect has come to an end, but the survivability clause says the agency retains the right to use that app after the contract has come to an end 100% Telice.

Megan Smyth: 31:30

You want to make sure that your IP clause clauses are included in your both severability and survivability. So what can these clear terms do? They can prevent disputes with the vendors and they're going to foster a better long term relationship. So what you've got to do here is a balancing act. Right, you are balancing the state's interest with your fair treatment of the suppliers, because you want them to innovate, you want them to compete with each other in a way that creates the best product for the state. And in order to do that, you've got to give a little too right? You can't say, well, you created this for us, it's ours, mine, mine, mine, mine, mine, and no one else can use it or see it or look at it. That's not fair, especially if they're creating technology that they can use in other instances that may have nothing to do with what they built for the state. So they created a code or a piece of software or something that then has another application in another industry.

Megan Smyth: 32:31

For another reason, we don't want to prevent, uh, innovation, creation and creativity in the in the public set in the private sector. Why would we want to do that? That would only hurt us in the public sector, who benefit from the products they create. So, in order you know, fair market capitalism, here we are. We want to ensure that for that transfer or commercialization of the innovations developed through the government contract. Now that requires some very clear terms and conditions. That requires some very clear rules about what you can and cannot do with the technology created, technology created. Now, following up on this and making sure people are doing what they're supposed to be doing is a whole other podcast, for a whole other day. But making sure that you're putting in the language to protect yourself in the instance that this occurs is important. You will be very glad that you did. You also want to consider things like data rights, security and confidentiality and future flexibility with the technology.

Telice Gillom: 33:57

I think a good example of technology transfer or commercialization of innovation developed through government contracts would be something like Velcro being developed for the space program.

Megan Smyth: 34:11

Yes, yes, I was going to say I think, and then commercialized for use.

Telice Gillom: 34:16

And now Velcro is on everything from shoes to pet jackets and wigs.

Megan Smyth: 34:25

Indeed. So when you think about building this clause, uh, as the attorney or as the contracting officer, you want to think about several things. Who owns the ip that has been newly created through the contract? Who owns the ip that existed when the company signed the contract with you? So they may have had their own intellectual property and you go to them because of that right. Oh, we know you do this thing, we want you to do this for us and they build something for you.

Megan Smyth: 34:58

The new thing may be owned by the state, maybe the intellectual property of the state, the old quote, unquote old thing. The existing IP still belongs to the company, and that needs to be very clear. What was created, what is new? And often you need to work with the supplier for them to tell you that you have to work together and understand each other and be willing to compromise with each other about this in order to get the advancement of technology that we want in the state. You want to be able to modify or distribute that intellectual property if it does in fact, belong to the state, so you don't want a requirement that you have to reproduce it in a whole in order to use it again. You may want to use a piece of it here, a piece of it there, but the company that created it may not want that. So that needs to be a piece of it here, a piece of it there, but the company that created it may not want that. So that needs to be a conversation. They could say we don't want you taking this apart and using it in other ways, we only want you to use it this way, and that can be a point of negotiation, a conversation that you have.

Megan Smyth: 36:02

And then warranties against infringement. Now, this goes several ways. You want the supplier to warranty to the state that they are not infringing upon any other company's intellectual property when they work for the state, because that can create a whole issue of liability right. Who would be responsible for that If the state is using intellectual property that was created for it by a supplier? State is using intellectual property that was created for it by a supplier, but the supplier stole it from somebody else. That's never a good situation. So you want a warranty, a guarantee that you can trust in from the supplier that they have not done that and that if they have done that, whether advertently or inadvertently, they're responsible for it.

Megan Smyth: 36:49

And then, finally, you want a disclosure requirement, so you want to make it clear what you need the supplier to disclose to you about the intellectual property that existed when the contract was created, versus what they are creating for you and this doesn't have to be super technical language, but it might be, depending on the type of contract. And what you want to do in that case is bring in an SME who can explain it to you as the attorney or the contracting officer. What's actually going on here, what's being created and what we are even talking about. So use your resources. There are some brilliant tech resources in the state. You can always reach out to your CIO's office or ask for help, because no one expects everyone to know everything when it comes to this advancing technology. That would be impossible.

Telice Gillom: 37:44

Megan, as always, I appreciate you chatting with me today about terms and conditions, our second in the series.

Megan Smyth: 37:51

Well, thank you for having me. I hope that everyone has gotten something out of this that they can take back to discuss with their colleagues or their friendly neighborhood attorney.

Telice Gillom: 38:01

We'll keep going in this series. This is part two of three, and we will see you on the next one. How about that? Sounds great. The comedy duo will be back again.

Megan Smyth: 38:15

Come for the information, stay for our corny jokes.

Telice Gillom: 38:18

We've got more. We'll have more corny jokes in store. I'll think of a really good one. Bye.