Di **[00:01:30]**: So we've been talking about some of the business drivers and the capabilities that GFIPM [Global Federated Identity and Privilege Management Standard in a Four-State Information-Sharing Enterprise] and the technical privacy framework enable. And those are very important in terms of making a business case for your stakeholders. But now, maybe what we can do is shift gears a little bit to how the CONNECT partnership has arranged itself for governance, development of policy. You've maintained this consortium for almost seven years now.

[00:2:00]

Tell us a little bit about how you're structured and how you come together to manage this project. Mike, would you like to start off? Who are the stakeholders from your perspective?

Mike: I think given the nature of CONNECT being a consortium of four states, we're fortunate that we had point people in each state: Maury for Alabama, Stephen Myrum for Wyoming, Steve Montgomery in Kansas, and then me for Nebraska.

And, when we started talking we knew we needed to formalize somehow. And so, we decided to go to basically a policy type board and try to set up a structure that would allow us to meet regularly, hopefully, and make decisions regarding things. As Maury mentioned, we knew right away that we had to address upfront – we couldn't just start coding right away and start sharing data – we knew we had to have a structure for doing all of that. And we wanted to be able to be flexible, to be able to expand over time, add data over time. But, it was more important than, I think, formalizing and documenting that trust –

[00:02:59]

and knowing that it wasn't just a board or a project – ultimately, we were going to need to extend each of those relative to the nuances of certain data. That, whatever we were sharing, might have different needs, or requirements, or MOUs [Memoranda of Understanding].

And I think one thing that's really important is that while we had four different states, we all had our data portals. And so we had a governance structure within our states to oversee the use of the data to even allow this initiative to go forward. And so that really

gave us a basis for being able to talk to the other states and be able to look at the data.

And I think that's incredibly important: everybody needs to govern their own data for their internal use, for their own project, whether it be at a county level or a state level. But that gave us a springboard to be able to look at what the differences might be if we wanted to share with a different state or multiple states.

Maury: It took quite a bit of planning, because we had to go back and look at the way each of our states form our legal authority to do what we all ready did.

[00:04:00]

As Mike said, one of the nice things was we were the point people within our states to come forward with this as a driver. But we also had our own mechanisms within the states. In the case of Alabama, I'm driven by a commission of officials, and we presented the idea of CONNECT to them and it was a formal vote, a regulatory body for the state of Alabama deemed, "Yes, what you're doing is appropriate and valid and we give you authority to do this."

We had to go back and look at the way we have documentation out to the user base, which is pretty broad. They already have to agree to security provisions when they are connecting to our in-state portal. But, one of the keys was, this is a broader project than just in-state. So, we modified our security agreements.

[00:04:57]

They all, now, any officer – any ***user,*** because it's not just officers, a court official, or a DA [District Attorney], or whoever – every time they log into the system, they're also agreeing now to the broader provisions of CONNECT. So we've covered the policy ground and it took backing up, looking at our internal systems.

Now, at the national level, at the CONNECT Board level, we created a Board, a governance Board, and we also have a set of bylaws that we all agreed to. It was not easy to come up with that – it was a labor, but it was an important labor. So we went through and have detailed guidance for all of us on how we're going to deal with each other. And it was fully vetted by lawyers and everything, too. It wasn't just us, the four of us, coming up in a

room and dealing with it. I mean, there was a lot of structural process behind it. It took awhile.

[00:05:55]

Really, we have a great foundation now for expectations from each other, the way we're governed, and how we can rely on each other. This ***trust*** that Mike was discussing.

Di: John, when you look at the CONNECT governance, do you see any best practices there that you would recommend to others who might be considering a similar consortium?

John: I think the structure that they have formed of having a kind of an executive level governance board and then having delegated authority to the various CIOs [Chief Information Officers] within their organizations to actually then do the information sharing is a structure that I've seen in JNET [Justice Network] in Pennsylvania. I'm down at the county level, the County of Los Angeles, but the County of Los Angeles is pretty big, bigger than a lot of states. And we operate similarly.

[00:06:57]

We have a countywide criminal justice coordinating committee that has the department heads of all the major county organizations, plus we have local police chiefs on that committee. We also have federal officials, as well as the California State Department of Justice officials on that committee. And we meet monthly and when we want to do an interagency-type exchange, they've already, you know, basically supported that particular method and delegated the authority to the organization that I'm the director of: the Information Systems Advisory Body. And we actually then go out and get the technology and we get the agreements, etcetera.

So, I think you definitely need the executives that understand the business issues and the legal commitments to share the information. Then you need that next layer that can get down to the technical layer and really look at the policies and look at the attributes for how you're going to accomplish a federated exchange.

[00:08:01]

I just want to mention that, as far as regional sharing in L.A. County, we're probably still not as far along as CONNECT, in terms of information sharing with the surrounding counties of San Diego, San Bernardino, Riverside. Within the counties, San Diego's done a lot of work and L.A. County's done a lot of work for sharing amongst the local agencies. But moving across even those county boundaries is something that we probably need to form something like on a smaller – I don't want to say it's a smaller scale population-wise; it's maybe a ***bigger*** scale – but something that brings the various county jurisdictions [together], because crime sees no borders.

Maury: Same paradigm.

John: Same paradigm. So, I basically endorse that the model that they've done is pretty successful –

[00:08:57]

– in our organizations, as well as some of the others . . . . I should mention the National Information Exchange Federation [NIEF] that the [United States] Department of Justice, using the Global standards, we formed this, and L.A. County participates in that. And we have a template for a governance model of a federation and a template for the policies and procedures and responsibilities. We're adopting those for our own internal federations.

I know that CONNECT did the same thing: when they went to actually do the technical work and the internal policies and procedures for setting up a federation, their vendor used those same templates. So there is some guidance out there and documentation to help you formulate the governance structures for information sharing – ***secure*** information sharing using the federated model.

[00:09:58]

Di: Good. There's no reason to reinvent the wheel. There's a lot of good material out there to reuse. That's good. Now Mike, Maury mentioned that he needed to go back to his Criminal Justice Information Center's governing body and seek approval for participation in the CONNECT project. Did you have a similar experience in Nebraska? How did you formalize your ability to participate?

Mike: Initially, we have a CJIS [Criminal Justice Information System] advisory committee that involves the state and local criminal justice shareholders. And so we presented this as an option to them first to get buy-in. Originally, it was really conceptual: we didn't really know if it was going to work, if it was going to go on. The term "federation" hadn't even been floated around. You know, we were just trying to figure out a way to do the technology. And they were for it: they saw the benefit of going beyond the borders. But, to me, the next step beyond that – and John kind of alluded to that – is the datasets themselves.

[00:10:58]

Mike: When it came down to the details about what could be shared relative to DMV [Department of Motor Vehicles] data or court data, or whoever, we weren't going to make assumptions about what we could do. Just because we could share it within our state, we didn't know about any nuances that might exist about going beyond that. So we made sure that we got the buy-in from the data owners, the people that maintained the data itself, so that they could really say that it was okay to share the data with, eventually, maybe L.A., or with Alabama, or with Wyoming.

We don't want to lose that notion. We at NCJIS [Nebraska Criminal Justice Information System] really just broker the data. We act as a way to get out the data. We don't really own much data itself, or ***any*** data itself; we provide that mechanism to share. But I think if you get out of touch with the people who really own the data and maintain the data, that's where you can come into some problems.

Interviewer: That makes a lot of sense, Mike. So was there formal Nebraska legislation, or was it the idea that the Nebraska legislature has delegated to your advisory board the authority to make these decisions?

[00:12:02]

Mike: The legislature set up the advisory committee without necessarily the details to allow this, but to pursue data sharing and data integration. And the NCJIS project itself came about because the data owners were willing to sit at the table and agree that sharing data made sense, and so we did MOUs with all of the participants, both at the data provider level, as well as at the data consumer

level. So the agencies that have access knew what the restrictions were, knew what the guidelines were, knew what they could do. It's really driven by the people that are at the table more than the legislation, actually. The underlying legislation says what the data can and can't do, what an agency can and can't do with it. But, it doesn't explicitly talk about all of the mechanisms to do that.

John: I'd just like to second that, that the legislation is actually something you consult when you're actually doing the particular exchange –

[00:12:59]

– but the decision to do the exchange and the authority, if you will, is not by legislative act. It's really by agreement between the various department heads and stakeholders. And then you consult the legislation to see what parameters around that information exchange are permitted.

Mike: Let's talk about the courts. I mean, we've got several branches of government, as well. So you've got the courts on the one hand, those executive agencies at the state level under the governor, and you have the local agencies, police, sheriffs, jails, and everything else. So, there's a lot of different dynamics going on.

Maury: I'm thinking in terms of the way our structure – I had agreements in place that allowed us to take driver's license information. And as long as we applied the particular security policies that we do and it's for criminal justice purposes, and it meets all the guidelines, sure, we can do this just as well through CONNECT as we could possibly through NLETS [the International Justice and Public Safety Network], or NCIC [the National Crime Information Center], or other methods.

[00:14:04]

So they gave us that flexibility with the MOUs all ready in place within the state. And corrections data was the same way for Alabama. So that's one reason we were able to bring this to the table so quickly because, as long as we followed the guidelines all ready set in place for sharing, security models and so forth, then we're good.

Di: That's great. So now imagine that one of your state partners, let's say Kansas – let's say that the Kansas legislature amends that

statute that governs access to a particular piece of data, either broadening it or restricting it in some way. How does CONNECT enable Kansas to maintain its own governance of its own data within the CONNECT partnership? How does that play out? Do you want to take it, Mike?

[00:15:05]

Mike: That's part of the natural extension of the technical standards – GFIPM and PEPs [Policy Enforcement Points], PDPs [Policy Decision Points] – a lot of the privacy extensions of being able to describe the type of data, who can have access to the data, and the use of the data that gets buried between the authentication as well as the types of validation and types of authority that are passed based upon the user credential that goes through GFIPM. It's a fairly complex technical underpinning. But it really allows you to define all of that.

So if things change for Kansas, they could go in and redefine that technical standard, pointing at what types of users could be used. Now, the thing is, you can't anticipate all of those things, so you can't build all of that in up front. You might be able to take away something that you build in. But if all of a sudden the legislature talks about a new type of user – and we've talked about everything from fusion center types of folks, to DMV folks, to corrections folks, to whatever might define who has access to the data – you can't build all of that in up front.

[00:16:04]

You have to be sure, and even if you could build that within the technical structure – to restrict another state's users – the other state has to be able to pass that information on to Kansas so that they can verify that they know enough about the user trying to look at the data to be able to make that decision to either allow access or not allow access. So I think the technical standards allow for that. But it's not totally comprehensive, out of the box. You have to be able to adapt and keep making changes.

Maury: I think you can go in and presume there are going to be changes –

Di: ***Presume*** that, yes.

Maury: – that there is a constant evolution in the way we share data. And generally the evolution is getting to it's a broader sharing

environment, but that isn't always the case, especially with more concerns about privacy. We're getting to where a lot of data is available and accessible, especially internally.

[00:17:00]

Every time I talk to Mike, they've added a new dataset, there in Nebraska, and in Alabama as well. We're constantly consuming internally. Well, we're having to evaluate each of these now in a broader perspective of the nation through CONNECT. And, we're not there locally, internally within the state on moving everything forward. It's just a piece by piece because we really need to look at the data and see how it can evolve into the bigger picture.

I do see it going there. I think we've created a construct now that is very versatile. The thought process and the maturity now that we've moved to especially with the GFIPM 2.0 model creates all kinds of possibilities for us to be creative in our own states, to have diverse standards or, well, that's not the right word, diverse authorities and permissions that –

[00:18:01]

– that translate differently in other states. But the technology can handle it, which is pretty exciting when you get down to it and see what's possible now. This does lead to the idea though that there's as much work on the governance policy side as ever in order for us to make sure we've thought through it well to apply these technologies. So, I think that's where we are today.

Interviewer: So just to extrapolate from a couple of the things that you gentlemen are saying, what I hear is that it is impossible to predict all of the datasets, all of the potential requestors, all of the potential information sharing partners. And so these standards enable you to expand and adapt to changing policies. Is that fair?

Maury: Well, I was thinking, it's –

[00:18:59]

– the user, the diversity of the user base, as well. I mean, there's so much, there's all these different pods of considerations you have to take into account, but yes, the technology is there to allow us to look at the type of user, look at the type of law governing the type of data, and the exchange that goes on and it –

Mike: That's also because the standards themselves are evolving, right?

Maury: Exactly.

Mike: When we started out . . . . You mentioned 2.0. When we started out, we didn't know there was going to be a 2.0 or 3.0 or whatever.

Maury: Or a one-off.

Mike: Or a one-off – really! Good point. So, you take the standards as they are. You try to implement them. You try to expand them. You try to understand them in the first place, with the acceptance that they're going to evolve because people are going to find need.

We're going to find that we need to do something else and the standards need to evolve. Things within the standards come together and evolve better. So sometimes people ask when will the project be done? *[laughter]* And it's not going to happen. It keeps changing and that's a good thing. If it didn't, we'd be in a problem.

[00:20:02]

Di: That's what puts the "extensible" in the standard, right?

Maury: Sure.

Di: John, from your perspective, do you have anything to add to this idea that the standards themselves are evolving to enable new partners and new types of data?

John: Yes. I think the standards are definitely moving forward and recognizing that underlying what we've done in this framework – "we" being the standards industry, not we here at the table – is that when we centralize, if you will, your vetting of your users and the information about those users, and transmit that as a credential to another organization, that moving that away, out of your internal applications –

[00:21:00]

– gives you that flexibility and adaptability as new kinds of roles come on or new types of attributes you can add to the vocabulary for defining your users and their access to resources.

And then, on the resource side, moving the rules about what you can or can't do against this particular resource, what you can access. Having that external, as well, is giving you the flexibility to adapt it. You do not have to go into some application and change some VB code or some Java code, etcetera. You're really running a rules engine out here. So those are both flexible and support this evolution of new interfaces, new exchanges, new types of users, new types of rules, changes in rules. All of those things now you have a framework in which to work that you don't have in our classic model of building what we called, overused again, the "silo'ed application."

[00:22:06]

Di: Mike and Maury, do you have any memories of particular challenges in governance? Did you encounter some obstacles along the way over the past seven years? Anything you'd like to share?

Maury: Nothing just dramatically stands out as a huge challenge, other than it took a lot of time just to think through the process because we didn't really have go-bys at the time. I mean, when we were starting, well, there was some technical documentation, but when we think about the governance . . . . Really, when we created the bylaws, we just got in the room. We looked at CJIS [the Federal Bureau of Investigation's Criminal Justice Information Services] security policy. We looked at our internal state agreements.

[00:23:01]

We looked at our laws in our states. Sort of threw them all on the table together. We met numerous times. I remember going up to Nebraska and we went up to Kansas. We've had numerous meetings, whether it's in D.C. [District of Columbia] and different places, and a lot of phone calls, you know, and it took time. But we finally got to where we felt very comfortable. And I think we're proud also of the document. The document sort of binds us together now.

Mike: Because we were starting from scratch on both the bylaws and the governance, as well as on the technical side, we were fortunate that

the four states and their point people knew each other. And, I think, we knew that we wanted to make this happen. We wanted it to work. It wasn't, "kind of a good idea and we'll see what happens." We really wanted to make it work. And so that really helped us, I think, with the framework for doing governance and for trusting each other.

[00:23:59]

It would probably be different if you had ten people that were professionally familiar with each other and had all seen the same e-mail and seven of them showed up just to hear what's going to go on.

You need that commitment – I think it really helps. It was a collective governance approach, as opposed to trying to come out with an external federation that we all were trying to belong to, which is the more classic model on the technical side. So, I think that helped us, as well.

Di: Everyone was willing, everyone saw benefit for themselves?

John: I would just like to interject real quick, though, that's not always the case. In terms of governance, if the leadership of a particular agency, you know, is not the type who . . . [If] they're very controlling and it's, "This is my data –

[00:25:00]

– and you can only get to my data through my security and my mechanisms. And I'm not going to play." You can kind of expect that's going to happen. And usually, as in any consortium, there's usually at least one party that doesn't want to play –

Di: Some reticence there.

John: – yeah, and they all have their own authorities. That's a reality, too. Unless the leadership wants to do this, you won't be able to get there.

Maury: That's very important. For CONNECT – this does remind me, the memory is coming back – early on, we actually had six states at the table. And the more we moved through the process, we realized that not all states were prepared.

[00:25:57]

So, that's one reason there's sort of this land bridge between Alabama and then go over to Kansas, Nebraska, and Wyoming.

We know we're going to get there with other states. We've had so many states call us now and want to join, but we're trying to get the foundation very solid now and make sure we've got something that we can almost hand to them on a silver platter. And I think we've gotten close to that. We're about there.

Di: I want to explore this idea that the partnership itself is extensible. So walk us through what you imagine the process will be when a whole new state wishes to join your consortium. What will that look like?

Mike: Well, our discussion has primarily been that we want to add states. We want to add people that similarly have data that would be useful and that they can contribute.

[00:27:04]

But we also want to be sure that we have all the technical structure underneath. We've basically gone through two phases. Initially, we thought we would end up with something that was very driven by the state, very internal of the state, take a lot of work internally at a technical level to be able to join. And then we went through the second phase: we went to, as it was described, a more external approach, where it's more of a web, centralized type of thing that's going to broker a lot of the security stuff. And that's a nice model. It makes it an awful lot easier for someone to join.

And so I think, as Maury said, I think we're much closer to that and be able to do that as soon as we lock down a couple more things that we're able to do. And we've had people ask to join, who want to join, who want to add data sets. And we want to share our data with others. That's the idea. And, you know, we need to close the gap a little bit with some other states.

[00:27:59]

There's technical needs for somebody to join. There is going to be cost, but it's not going to be the same cost as going completely out of the chute in the beginning.

Di: How will you integrate new states into your governance?

Maury: We have the documentation now and we have the policy, the bylaws. Really, since we haven't done it, there's no way you can say, "This is the way it's happened." But the idea that we've discussed is that a state will review the bylaws and decide if they can meet the expectations that are in there. I mean, they have to have legal authority, have to have some kind of user management capability already in place . . . .

Di: An active directory?

Maury: Of some sort, yes. And then be willing to make the changes internally, whether technical or policy-wise because I think all four states today –

[00:29:00]

– actually did change internal state policy to some extent to work on the big picture. And so they'd have to do that within their state. But once that's done, I think we would be very willing to accept them into the pool. I mean, we welcome that, we want that.

Mike: Right, and we envision the Board itself expanding. I mean, [new] people aren't going to be secondary.

Maury: No, no. Everybody would have an equal voice at the table. It's not supposed to be confrontational. I mean, it's that idea that we are committed, I mean to me that is, I love that term, how it gets used because it is so important. It's the commitment of the states to get their data out there and let's share it in new and exciting ways that we haven't had the possibility of doing before to a broader audience than we've ever had before and in a more secure way. So we're going to have that soon.

[00:30:03]