Department of Justice (DOJ)
California Law Enforcement Telecommunications System (CLETS)
Standing Strategic Planning Subcommittee (SSPS) Meeting
November 13th 2023
10:00 a.m. (PST)

Meeting Minutes

Agenda Item #1: *Meeting was called to order at 10:00 A.M. by* ***Ashish Kakkad.***

Agenda Item #2: ***Ashish Kakkad*** *took roll call. Members present included:*

1. **Ashish (Yosh) Kakkad** - SSPS Chair, San Diego Sheriff's Department
2. **David Angulo** - Department of Motor Vehicles
3. **Kirk Beardwood** - Department of Justice
4. **Timothy (Tim) Craney** - Riverside District Attorney's Office
5. **Kim Honciano -** San Mateo Police Department
6. **Justin Riedel** - Sonoma County Sheriff Office
7. **Adam Vallejo** - Riverside County Sheriff Office
8. **Tracy Weber** - Menlo Park Police Department
9. **Joey Williamson** - Hillsborough Police Department

Members not present:

1. **Lisa Marie Gerard -** San Francisco Department of Emergency Management
2. **Laura Cerda** - California Highway Patrol

9/11 members in attendance, quorum is present.

Other Subcommittee Non-Members present:

1. **Chris Blair** - SSPS Staff support
2. **Milad Dalju** - DOJ CLETS Legal Counsel
3. **Lydia Shindelbower** - SSPS Staff support

Members of the public who made comment:

1. **Kimberly Grimm** – ACC, Riverside County Sheriff's Office
2. **Greg Park** – IT Coordinator, Livermore Police Department

Agenda Item #3: *Housekeeping. Mr. Kakkad advised all attending the meeting that the meeting was being recorded.*

Agenda Item #4: *Vote on last meeting's minutes.* ***Justin Riedel*** *voted to accept minutes from June 20, 2023 meeting, and* ***Adam Vallejo*** *seconded. Minutes were approved.*

<u>Agenda Item #5:</u> ***Chris Blair*** *provided an update on the modernization of the CLETS application process.*

Mr. Blair: There is no major update at this time. We have moved to a new bureau and we are working with new management regarding the modernization of the process, as well as other systems. We're looking at an internal ticketing system that can produce consistent results from the analysts, as well as combine the app and security questions into one document to make the process more efficient. We currently have a few agencies testing the document, so we are gathering that feedback. We are hoping to have that document ready to publish within the next few months. We don't have a precise date for that, but I want to assure the group & CAC that CAS is working in a positive direction regarding the application process.

Mr. Kakkad: How many apps do you get annually or monthly?

Mr. Blair: At any given time, we can be working on 30 or more. As some are approved, others come in. As for the total, I think we have 10 or 12 upgrades that have been approved since the last CAC meeting and a number that are still in process.

Mr. Beardwood: CAS is under my responsibility as of October 1st. They've done a great job so far. We believe we are going to make some massive improvements and we can give you more accurate stats by the next meeting. I will take that down as an action item – the average number of applications we work on at any given time.

Mr. Kakkad: Between us and DOJ, we can identify resources that DOJ needs to allocate to this process improvement. Anything we can do to work together to document it and put together those recommendations for CAC will be huge. This is one of the items that we make sure goes into SSPS recommendations as part of the SSPS Strategic Plan. I'm happy to hear there's a lot of work in process already. Anyone on the call from the SSPS side have any questions, comments, or thoughts on this?

Hearing no comments on that item, I'll open it up to public comment.

Mr. Park: Thank you, Chair. This is Greg Park. Great to hear that DOJ is working on that update. Can you please provide a courtesy copy to SSPS and CAC so we can review what those changes are? That way we can provide some input for upcoming meetings. Thank you.

Mr. Kakkad: Thank you, Greg. Any other comments from members of the public who are on the call?

Next up is another update on the NextGen 9-1-1 feasibility discussion. Thank you, Joey, for getting more info from CalOES on the current state of NG911. Can you please give an update on what you found?

Mr. Williamson: I sent them a list of questions regarding the bandwidth of the network, the bandwidth of each PSAP, which is 10 megabits per second, unless it's considered a large PSAP,

which will be 100 megabits per second. I asked them about improving the system with bandwidth increases, and they will increase as necessary down the road.

Most agencies have two circuits coming into their PSAP, so I asked if those will be integrated into each other to increase bandwidth during peak traffic? They will all work together to share the bandwidth during high-volume times. I didn't have the specifics from DOJ regarding the amount of data going through, but I did let them know that there were approximately 84.8 million inbound messages and 85 million outbound messages going through the CLETS network, and I asked if they had any concerns regarding that impacting traffic on the NG911 side of things. They said that would have to be determined on a priority-need basis for each message. They'll need to meet & discuss the additional messages to see what kind of priority they would have.

I did let them know that, with CLETS, there is a lot of sensitive information going through that needs to be protected, and we may have different encryption requirements on the DOJ side versus the CalOES side. I was asking what the current encryption level of the NG network is, and would they change certificate levels as more security requirements are introduced.

They said that the NG network is currently using TLS, but they were unsure of the level at this time. They would need to reach out to NG vendors if increased encryption is needed down the road.

The last question I asked was if they saw any issue with non-PSAP agencies accessing the network, because we know there are courts, DAs, and others access CLETS. But they would never have the connection to the NG switch. They said that would be a policy question, and they would need to have the NG network tariffed and regulated – they will need to discuss that internally.

That's all the information I have at this time. I know Yosh reached out to DOJ regarding the NG network, because they were not aware of how far they'd come along with that network.

Mr. Kakkad: I want to thank Kirk, Chris, and the network folks at DOJ. We had a really good call and based on the conversation we had, there are some network upgrades that are in discussion at DOJ.

Before I dig too deeply into that, I want to open things up to SSPS to get their thoughts.

Hearing none, I think based on the information that we've gathered from CalOES, based on how the technology and strategy of how locals are deploying, we need to have a serious discussion about what the next generation of CLETS will look like, or what that could deliver. I'm not convinced that NG911 is it, but we definitely need to discuss it further. I see an opportunity for us to modernize and support DOJ in their modernization effort of their backbone infrastructure. Workloads are transitioning to the cloud. Access to CLETS is really holding organizations back, and the infrastructure built out by CalOES for NG911 at least provides us a robust blueprint of how we could look at it from CLETS' perspective. That's my thought on it. What does everyone think on that?

Mr. Riedel: I think it's great to look at different redundancy options and get more information. I support that.

Mr. Kakkad: Our role as SSPS is to write these three points up as formal recommendations to CAC, and I'd rather not this turn into a forever discussion and would like to finalize some thoughts surrounding this particular topic and get our recommendation documentation moving. I see it having a significant impact for everyone involved. Any thoughts from the DOJ team?

Mr. Beardwood: Unfortunately, Yosh, my area of expertise is not networking.

Mr. Kakkad: Chris, can we get the networking team to give us a brief overview of CLETS future ideas and plans?

Mr. Blair: Yes, we can. I can reach out to them to see if they can join the next SSPS meeting.

Mr. Kakkad: I see that we really need to make this a huge priority so we can really take advantage of the modern infrastructure that is now available. That would be great at our next meeting. Any other thoughts from the group?

Mr. Williamson: I do think using the NextGen network is a good way to model what DOJ can do from the CLETS side, just because we are seeing it happen on a statewide level. It's good to see how it's going, as well as the hiccups. It's nice to see it playing in real time and to see what could happen on the CLETS side at DOJ.

Mr. Kakkad: We should keep our role in mind, provide our recommendations to CAC for their consideration. It's important for us to capture the totality of impact for something like this. Any other comments from SSPS members on this matter? If not, I'll open it up for public comment.

Hearing no public comment, let's move onto the last bit -- training regarding changes to CJIS Security Policy 5.9.2 and ongoing webinars. Adam, I'll put you on the spot for this. Can you provide an update?

While Adam works on unmuting himself, I think what it boils down to is that we need to know if this is particularly important to the team. Maybe have us make a recommendation as part of our SSPS update to the CAC to say DOJ needs to provide quarterly or yearly updates regarding the impacts of these changes, a better understanding for agencies of when they need to submit their upgrade applications and what that looks like. If the group here recognizes that as a priority, Adam & I can put something together as a recommendation to the CAC.

Mr. Williamson: I believe that's a good idea. There are a number of Agency CLETS Coordinators who have recently retired, and incoming ones are very clueless as to what is required of their agencies. Some of them have even been asking what a mnemonic is. That type of information wasn't passed down in their succession plan. Further education for them would be really helpful.

Mr. Kakkad: As quickly as CJIS security policies are changing – especially the number of changes on the technical side -- I see this as two-pronged. Both the ACCs and the technical staff need to be aware of the changes. I think these webinars will be beneficial for both parties. It will also allow us to mitigate, streamline, and clarify the message to the agencies versus the vendors, who often control the narrative of what's required within the CJIS Security Policy. Thoughts on that?

Mr. Beardwood: Just to clarify for me, you're asking that DOJ create a bunch of webinars? Is that what the ask is? They would contain ACC training, what the ACCs are responsible for, as well as updates to the FBI CJIS Security Policy? Is that what you're thinking these webinars would be about?

Mr. Kakkad: Yes, that and knowledge regarding ACC responsibilities is really going out with the retirements. Another piece is: as new updates to CJIS Security Policy are made – multi-factor authentication, cloud aspects, etc. – the agencies need to know what those updates are and how they impact the agencies. It's one thing to give them a 350+ page document and say, "You need to comply with this." It's another to have a dialogue, to have messaging from DOJ that says, "This is what it means to you guys, as local agencies."

Mr. Beardwood: How would DOJ know your infrastructure to tell you how to replace your controls? That's your responsibility. I'm just trying to see how DOJ is supposed to interpret the FBI policy for you without knowing your end. I'm really struggling with that, I'm not trying to be a jerk here. The FBI policy is pretty crystal clear about what needs to be done, you own your technical system, and they tell you what needs to be done to your technical system. I'm just not too sure – I'm just trying to understand what DOJ's role would be without me saying, "Yosh, you need to use this control, this control, this control…" and you say, "Kirk, I already have those three controls, plus two others…"

Mr. Craney: I don't know that I agree on the "crystal clear" part. I think that's the part that Yosh is getting to. It may be crystal clear to you, but when you say "crystal clear" that way, we don't see it that way.

Mr. Beardwood: My apologies. It's not crystal clear to us either, but I'm just trying to understand how DOJ takes their role of transposing somebody else's policies. We've been having discussions about the same thing here, and -- my apologies, I didn't mean to cut you off.

Mr. Craney: When you say "crystal clear" like that, in the context in which you used it, we don't see it that way as the customer. That's what Yosh was getting to. We're just trying to get some clarity so there's less time spent by all of us trying to get things in place.

Mr. Kakkad: Thank you for that, Tim and that you for that, Kirk. This conversation here itself highlights the issue. We're not expecting DOJ to say, "These are the controls." We're not expecting DOJ to know our environments. We're expecting DOJ to have a discussion to outline the differences between versions 5.9.1 and 5.9.2 and how does DOJ interpret those controls. We don't expect DOJ to say, "Hey, this is your environment" – it's more about streamlining and getting DOJ and locals on the same page.

Mr. Riedel: I agree with what Tim was just saying. DOJ has their auditors, they have a set of particular controls as part of their audit review process, and that is more generically what these new ACCs don't understand. Especially since there have been such extensive changes. It's a lot more technical now. I have a CJIS background, so I understand what's in that document, but based on talking to my downstream agencies, a lot within my county don't even really know what multi-factor authentication is. Most of them kind of know what that is, but some of them don't. I think, in general, if you hand someone the CJIS Security Policy, they're just going to get lost. I hate to call it

the Cliff's Notes version, but it would be great if auditors from the state could come out and just say, "OK, let's look at this, then let's look at this…" to just boil it down to the key points that are part of the review process for them, that's what I think Yosh and Tim were getting at.

Mr. Kakkad: Thank you for that. Kim, you had your hand up?

Ms. Honciano: I'd just like to add, I'm with San Mateo County and as a medium-to-small-sized agency, we also lean very heavily on our county IT to help liaise with a lot of the networking and security components who also have lots of changeover and reassignments. Even though our ACC is longstanding and she has a lot of experience, and I've been here for a while, trying to explain those requirements to county IT who also have lots of changeover and have even less experience being directly engaged with CJIS, getting people into a meeting to have more open discussions and talk through some specific examples of what our infrastructure is and where our controls need to be would be really helpful, versus just giving them the CJIS document and expecting them to understand it point-blank.

Mr. Kakkad: Thank you for sharing that, Kim. I think it's a really good point for us to keep things in perspective. Kirk, I hope that sheds some additional light on what we're thinking regarding the value of these webinars. I think there's a definite need for us to come up with something to bridge this gap.

Mr. Beardwood: I don't disagree. I appreciate all of the feedback. I understand, I've had to read the policy a couple of times, and there are parts that are not my area of expertise – I'm relying on my network team and security team for certain items. It's good to hear a narrative about certain things. I appreciate everyone's comments on this, I really do.

Mr. Kakkad: I appreciate the dialogue. It can help us get some clarity regarding everyone's overall perspective, especially from those at a local level. Anything else on this topic regarding training webinars? The other piece that we see is there's always a debate around when we should put in for an application. That's a talk, locally, we have frequently. Is that similar for those of you at other agencies?

Mr. Craney: I would agree.

Ms. Weber: I would agree. I know we here in Menlo Park are looking at going to Office 365 -- we're changing from mobiles to tablets. We're getting what our vendor has, which is called IRIMS and it involved two-factor and everything. And rather than doing one thing at a time, I don't know if it's best to do one big one change versus a bunch of small ones. I don't know if that's the proper way to do it.

Mr. Kakkad: Maybe the seminars can just be once or twice a year. When does an agency need to put that application in? I foresee a situation that reduces the overhead on DOJ.

Mr. Beardwood: I don't disagree with that. The "whens," the "hows," the "whys" are what we're looking at it. I've heard these comments for a lot of years, and I know Chris has a lot of great ideas,

and we can see what in-house tools are available to us that we can use to streamline things, but I definitely don't disagree with the ask.

Mr. Blair: When it comes to when to submit an application, it never hurts to reach out to the county's CAS Analyst. It really does depend on a number of different factors. You can propose your changes and they may have a set of questions to determine if an application is necessary or not. There isn't a set template of when an application is required, unfortunately. I also wanted to note that the DOJ Client Services Program does provide ACC training, and that's available on the CLEW website. I'm not sure of the details, but agencies can reach out to Client Services Program if they have questions.

Mr. Kakkad: Good to know. I think you're right, Chris, as to when – I don't expect us to have a checklist, but as the technical environment changes, I think having DOJ open things up to local discussion one to two times per year would be helpful. Any other thoughts on this last item? Let's open it up for public comment.

Mr. Park: Feedback from the public, Yosh?

Mr. Kakkad: Yes, sir. That's just about where I was going to turn, so let's open it up.

Mr. Park: On the topic of webinars, I think DOJ is in an excellent position to map out a CLETS Application process webinar, an informational webinar including: "Here's an application. Question four relates to this section in the policy. Here are the details that you and your technology people at your agency need to be clear on. We at DOJ are expecting to see this in your application…" I think offering something like that twice a year would be phenomenal. I think it would go a long way in billing DOJ as the leader and expert in that process, and it would be great to give local agencies the chance to participate in that conversation. Thank you.

Mr. Kakkad: Thank you, Greg. That's a really good point. We have Kimberly Grimm on the call. You have your hand up, ma'am.

Ms. Grimm: Hi, my name is Kimberly Grimm and I'm from Riverside County Sheriff's Office. I'm the ACC for our department. I did take the ACC training offered through DOJ. It was helpful, but what I did find was that a lot of the information was out of date. I don't think it's outdated in terms of it being a long time since the content was updated, but rather that there have been a lot of changes in a short amount of time. I would just suggest to review the training that was offered already and fix it to reflect some of the changes that have occurred.

Mr. Kakkad: Thank you for your feedback and for the information on the freshness of the content. Any other comments? Before we wrap up, any public comment on any items from the meeting as a whole? Chris, am I missing anything before we adjourn?

Mr. Blair: Agenda topics for the next meeting?

Mr. Kakkad: I think we can keep the same three items. Updates, next time instead of an update on number four, we'll put it to a vote; and then we'll have an update on number two [Agenda Item #5]

and number three [Agenda Item #6] from the DOJ perspective. Number three will be an update from the network team at DOJ, and number two will just be additional detail regarding what this process looks like. And item number four [Agenda Item #7] we'll put to a vote the next time around.

Mr. Blair: Yosh, can you clarify regarding item number four on the current agenda? It shows as "Approval of June 20 Minutes."

Mr. Kakkad: Sorry, I was referring to the training changes.

Mr. Park: A suggestion from the public?

Mr. Kakkad: Yes, sir?

Mr. Park: Extend an invitation to the new CJIS chief.

Mr. Kakkad: Yes, we shall do that. Good point, Greg. Let's extend an invitation to the new chief.

Mr. Blair: Will do.

Mr. Kakkad: If there's nothing else, we can adjourn the meeting.

Meeting is adjourned at 10:45 AM.