Hello, and welcome to the State of 911 Webinar series hosted by the National 911 program.
My name is Sherri and I'll the Moderator for today's session.

This Webinar series is designed to provide useful information for the 911 stakeholder community about Federal and State participation in the planning design and implementation of next generation 911, or NG911 systems.

It includes real experiences from leaders utilizing these processes throughout the country.

In today's session. You'll learn more about the Department of Homeland Security Science and Technology Directorate's Approach

to NG911 performance along with an overview of the lessons learned in the California Office of Emergency Services or CalOES, NG911 lab

for closed captioning hover at the bottom of the zoom screen for meeting controls.

Then click the CC button to start viewing the captioning

for more information on national 911 program Webinars, or to access archived recordings or learn more about the national 911 program,

please visit 911.Gov. Feedback or questions about the webinars can be sent to national 911 team at MissionCriticalPartners.com

The national 911 program

would like to make you aware that the documents and tools section of the website has been updated with new resources and improved access.

911 stakeholders are encouraged to submit links and documents that would be of use and interest

to colleagues, including, policy documents, plans, reports across several topic areas, such as governance, management, technical, operations, and standards and best practices.

You may access the web page under the 911 system resources drop-down menu, or scan the QR code in the bottom right corner of this slide.

The National 911 program would also like, would like to invite you to visit the 911 telecommunicator tree of Life, and share the name of a remarkable 911 telecommunicator who has inspired you.

Share your story at 911 tree of life dot org to honor a special 911 telecommunicator who's making a difference in your community.

Please Note: that All Participants phone lines have been put in a listen-only mode. And this webinar is being recorded. To ask questions of our presenters feel free to take one of two actions.

Using zoom's Q and A feature located on the bottom of your screen in the meeting controls. Enter your question at any time during the presentation, and it will be entered into a queue.

Hover your mouse at the bottom of the page and

access the meeting controls or you can ask your question live

using the raised hand feature to request your phone line be unmuted. You will be called upon to ask your questions.

Everyone registered for the Webinar will receive access to Today's PowerPoint presentation and a recording of the Webinar.

With that I am going to turn it over to Brian to introduce our first speaker, Sridhar Kowdley, Brian. Go ahead,

Hello, everyone. Thank you, Sherri. In our first session today, our speaker is Sridhar Kowdley, technical manager of the Department of Homeland Security, Science and Technology Directorate, technology center. What Sridhar will be talking about today is how

all of the next generation 911 parts or systems will work together in our nation's, systems of systems, and will be ensured that they perform in the same set of standards and operate as our 911, next generation 911, systems will be needing to interact with all of the different technology.

Sridhar, I'll turn it over to you.

Thank you, Brian, really appreciate the introduction. Again, we're sort of at S&T. Looking at this as a national program. It's, although we are sort of

kind of leading it at the moment. This really is our collective program. It's the, it's the industry folks. It's the users, such as NASNA,

it's the 911 operators. The key point here is what we want to do is define an independence, independent program to ensure that the 911 systems and components built

by the industry is conformant and interoperable.

Um, what we don't want to do is essentially have a system, or have a number of systems out there that don't work together well, or cause problems

in the long run, and then have to implement costly fixes.

The other component of this is we will be working with our, with our fellow partners at DOD to also develop a fundamental cyber security component to this. It may take the form early on as best practices, but the intent is to

ensure that the 911 centers are secure and at least a level two. We're calling it a level two. DOD has many levels that you have to meet, but we want to provide some fundamental structure and guidance to make sure that the system is secure. Our next slide, please.

So the agenda is real quick. I'm going to go through a background

not necessarily provide a overview of the 911 system, but provide the, provide sort of

information on what it is, that how we are looking at implementing the program, how are we guiding it? And then to provide a little bit of detail in terms of the key partnerships that we are forging. How are we funding it? And again

I'll go through some of the acronyms later on. But

just to kind of let everyone know this is a joint program between DHS, DOD and the Department of Transportation. So what we are Truly building is a deep partnership to make this happen. next slide, please.

So, just to kind of give you a background. Who is DHS S&T. And what is our role? DHS S&T is the research arm for DHS: So we support not only um all of the DHS components. It just goes for ICE, border patrol.

In terms of providing fundamental R and D. But we are also support as key stakeholders. The first responder of community nationwide.

So we actually were formed: our office, which is the office for interoperability, compatibility,

was formed right after nine eleven to ensure interoperability across,

across the environment, especially after what the nine eleven Commission put out in terms of key fundamental issues. regarding interoperability, where you know certain sections of the public safety ecosystem, couldn't talk to others. So we have formed under title Six of the U.S. Code.

And we have three main tenets is that evaluate and assess new technologies in real-world environment

To achieve interoperability and emergency communications.

We want to be able to identify and determine the strengths and weaknesses of public safety communication systems in use. And then, finally, we want to evaluate and validate the advanced technology concepts and facilitate the development and deployment of interoperable systems. Again, the focus here is to enable

and facilitate interoperable communications nationwide.

So, next slide, please.

So, one more kind of background for S & T: So DHS S&T is the program of record for Project 25.

And so a lot of what we're going to discuss today is based on the Project 25 program that we ensure compliance and interoperability for all land mobile radio systems that are sold in the U.S. Now, again, it's a voluntary program. However,

most of the major manufacturers go through our program to ensure that their radios are compliant to the standards and interoperable.

So, with regard to the NG911 system. I'm not going to go into heavy detail, because you guys know this better than I do. But, obviously,

why DHS got involved, and why we are involved now is now that the NENA i3 standard is been ratified by ANSI, and is pretty much the standard that will be used for all 911 systems nationwide at the moment.

So we decided to sit together and put a program of record together.

This program was actually initially funded through discussions with the 911.Gov program lead at that point with Laurie Flaherty, DHS CISA, the Department of Justice as well as DHS.

Other DHS components got together and said, Hey, we really need to solve the interoperability challenges that are coming down the road. Given that the systems are being developed now that the standard has recently been ratified.

So we were kind of trying to figure out how to do this. So in 2019 DHS and DOT, and DOD essentially later, got together, and we found some money because we really didn't have any funding at this point. So we funded the first phases of the

the program to really identify and approach

to identify, a methodology as well as a framework. For how would we set up a interoperability and certification program? What would be the key tenants?

How would we administer the program? What are the key requirements that should be built in? So we developed that framework with co-funding from DHS S&T, as well as department of transportation.

So we put this program together and kicked it off back in 2019.

We modeled the program on the P25 program that I just mentioned before, and there are some, some lateral initiatives that are very similar in terms of the approach. However, everything's in flux.

Part of the, part of the requirements would be, Since this is a

a program that's still maturing,

we'll have to work out some of the details, and there will be compromises that may have to be made based on specific testable requirements. How expensive is it going to be to implement, et cetera?

We have strong industry engagement from NENA, NASNA, iCERT and APCO. And there's more about this to follow.

The Federal stakeholders in this program currently are DHS S&T, DOT,

DOD, CISA, DHS CISA, as well as we're looking at NTIA and FCC. We had conversations with the FCC, and they're very interested in learning more about the program and seeing how they could support us.

Obviously, we want to get the program kind of kicked off and moving before the

funding comes out of Congress to upgrade 911 systems. The intent here is, we'd like some sort of certification program to be in place. So as people start developing and fielding these systems, there is a capability to say,

Are these systems really interoperable? Do they really meet the standards? Are there any technical issues that would prevent interoperability down the road?

Next slide, please.

So how, What are the key requirements for the certification? This is our current view. We want to do develop the test requirements. Part of those are already done.

We want to do up the test documentation. Everything from, you know, how what do we test? How do we test? What do we deem as a successful test or a failed test?

We want to be able to certify independent laboratories

to be able to assess and conduct the certification process. We want to be able to conduct the testing, and we think conformance and interoperability in the conformance piece we're really looking at, you know, do the subcomponents, the, the

systems to subsystems interfaces as well as entire end-to-end systems meet standards. Specifically, what we're looking at is kind of walking through the requirements that are built into the anti-standards

and part of the conformance testing that we want to do. We really want to build on the great work that Budge and some of the other folks have been done, doing, as well as the NENA the ICE work that was done for testing

911 systems, both domestically and internationally. And finally, interoperability, interoperability really looks at, you know, if I have three sub-components within an NG911 systems

are each component, can it talk to the other component, and the relationship between the two, and interoperability is really looking at

ensuring different manufacturers implementations are indeed interoperable and work together.

The governance team, which will be from our program office, and we're suspecting that that might be a partnership with DOT, DHS and NTIA

as well as some others, would actually review the test reports and approve the results.

And then we want to create some sort of website where users and procurers, people who actually procure these systems, will actually be able to go to a website and say, Okay, well, which of these manufacturer equipment and solutions have been tested?

And can I see the reports or the results of the testing, and we're not going to give proprietary information on this website. But,

what we would be is, here are the test cases that we successfully ran: Here are the reports that essentially substantiate those results, so that if anybody wants to procure or buy these systems, they have a fundamental confidence that they have been through a rigorous, well-defined, repeatable test program.

Next slide, please.

So we talked about interoperability. At the moment, um, you know, we are really thinking maybe we need to have a rule of three, where three different implementations have to be tested, to be ensured to be interoperable. Obviously there are certain challenges with this. The question is,

you know, how feasible is it to test three different industry solutions, or three different entire systems? Is that feasible? Is it possible? At this point we are not one hundred percent sure. You know the cost basis. All of those things have to be kind of figured out.

And whether the test labs, ah, if you can't certify any laboratories to do the testing, then you don't have a program. So there might be some compromises that we'll have to work out. We're actually trying to figure those out as we go. And obviously one of the things that we want to do is actually see if there's a,

there is a legacy support for backwards compatibility with existing 911 systems. And, this is especially going to be critical as we transition, because we're not going to do a forklift replacement for everybody all at the same time.

So we do want to look at the legacy, and we do want to look at multiple vendor solutions. Next slide, please.

So here's how the program is going to be worked, and it's going to be structured. It is going to be a voluntary program.

We at the Federal Government level can't

force vendors to go and test. So what we do want to do is, is in terms of carrots and sticks. We want to make sure that vendors who go through the program, we're going to, we're going to recommend that any Federal grant dollars, such as the ten or fifteen billion that Congress is going to allocate,

if you want to access that funding. And we'll have to work through NTIA and FCC, and a lot of Federal

agencies to figure out what language and how do we promote that? But the idea is that

those who want to use that Federal Grant dollars should go through the program.

And whether that's a should or a must or recommended, we'll have to work through the details on that.

Again, we want to encourage public safety acquisition programs, federal, State, local tribal, to make sure that they go through the certification program, or at least, are guided by the program before they

they do procurements. And this is going to require a lot of help from the participants on this, on this Webinar! Specifically, we want to know that you guys know that there is a program of record that we're standing up. And you guys

need to go and see if there is a testing capability and or results that they, you, can leverage before you buy equipment.

Now, it is important to note. You know we're looking at a eighteen month to two-year runway to build the program out. So in the meantime, you know, we're going to try to develop some documents that that you folks in industry and users can use.

Specifically saying our testing programs will use these kinds of test cases and things like that. So we want to make sure that the program has some aspects of it that can be leveraged shortly. And then, as we stand up the program, you'll have a false certification,

procedure or framework for you to follow.

The third or fourth bullet is really sustainability. What DHS is perceiving is that we will fund the development of the program in standing up the program. But long term we're really expecting the program to be sustainable, that vendors would either pay

the certification labs and or have some sort of monetary

payment to conduct the certification, and that would keep the program sustainable in the long term.

Our key requirements are, we're going to be transparent. So anytime DHS and the Federal agencies together, who are really the governance structure for this program, anytime we make rules or policy, we want to make sure everybody knows what it is. We'll give everyone a chance to chime in, and

respond with comments and suggestions, and then we will put the policy out for broader use.

We actually want to develop a governance policy that is tied to DHS

and Federal Government use. And then there will be also a technical policy that looks at, you know, specific triggers that we need to think about. Such as, How often do you test? Do you test every patch, or what is the minimum set of tests that you can do?

Those are all considerations that we'll have to put together in a policy, and we are going to be working on that, together with industry as well as users and

the broader stakeholder group. Next slide, please.

So who are the stakeholders here? We can't do this without all of you folks. We can't do it without the Federal government engagement specifically Department of Transportation, Department of Defense, because they both have a need, and what we want to do is, address

the broader need in one shot.

So that a vendor has very clear defined tests criteria to say, Hey, if I'm going to sell to the Department of Defense, or I'm going to I'm going to sell nationwide, or you know, here's the requirements that I have to follow.

We want to make sure that's clear. So the vendor community knows what their role is, what their requirements are and what they need to do in order to sell equipment.

We certainly expect the 911 partners to be key, front and center specifically, NENA, NIOC, NASNA, EENA. So

we've already reached out and worked very close to NENA and NIOC and NASNA. We actually had members of NASNA during the summit, which I'll talk about, that we had in the month of August. Obviously users and industry

are key program stakeholders. Next slide. Please.

So we've developed the three-phase approach. The additional slides below are going to be a little bit more detail, but I'm going to skip around a little bit and then give some time back for Q and A.

But um phase one is completed where we did operational technical requirements, gathering and stakeholder engagement with industry users, and 911 operators. In phase two, we are actually funding the development of a lab. That will be ISO certified, um Specifically what we mean by that is

a certification body will come, take a look at our testing documentation

and set up the first lab to allow testing.

So that level of effort DHS is already engaged in, and we're finalizing the funding right now for that.

In phase three, we're actually going to develop test suites, scripts and kick off the program launch. So this three phase levels, can you go to the next slide, please?

And I'm going to probably start skipping a few slides.

So in phase one really what we've done is

really developed a detailed list of test cases. We've actually worked with NENA,

NIOC, and some of these other folks to develop the first draft of it. If anybody wants the document, if anybody needs to look at it or contribute to it, that would be great. In terms of operational test or interoperability testing, we've developed eight test cases,

and obviously this as a very early release. We really need the help of folks on this call. If anybody wants to partner with us or help us refine the test cases and our requirements, we're happy to kind of engage with you guys to do that.

Phase two is currently in progress, as I had mentioned before. We're actually going to see if we can develop a laboratory with office of university programs within DHS. S&T is leading the effort.

We hope to build two fully capable 911 centers in Texas A&M. That would be the basis for the lab, and to actually work out the kinks in terms of how we stand up and operate on this program.

Phase Three is going to look at, what we want to do is develop an open source repository to allow all of the great work that NENA, NIOC,

EENA and ICE have done, and sort of leveraged that as a key point,

create a repository for

the software scripts that we would actually use in certification and make that open source. So that vendors and other people alike can use these tools to make sure that as they develop new products, new suites or updates, they have access to testing tools to make sure that once they come to certification,

not only are they going to pass certification because they'll have the ability to conduct these tests in their lab, it also builds in cost efficiency, so that vendors don't have to wait for a formal event to be able to have some level of confidence that they've built it right.

And, thirdly, um by allowing us to do this, we think we can streamline and reduce development time by

by providing these tools out there that that industry and users can leverage.

So um the last part of the document, the last phase is really the ongoing operations and maintenance for the program.

You know. How do we fund it? How do we continue to update it? And right now our program is focused on the actual ESInets and the 911 systems, but in the long term, obviously, CAD to CAD interfaces are, are

are, um, require some level of interoperability to be included, and what we want to do is, is focus on the NENA i3 standard for the moment. But we are planning on expanding the program in the future to take it all the way from

a 911 call being generated at a network, or on-star or some sort of automated process, coming all the way in, and then being able to push the data out. So we want to do this in phases.

And right now we're focused on the NENA i3 standard and the interfaces. So I think we can quickly jump through, Sherri, If you don't mind,

just kind of go through the rest of the detail slides.

Yeah, this is just a little bit more detail. These are some of the deliverables that we're looking at, and you know we sort of put this together, and we're using this particular

PowerPoint presentation as a way of

developing our tasks and requirements. But our intent here is, we want to leverage the fine work that NASNA, and NENA, and NIOC, ICE, have all done.

We want to sort of kickstart this process by leveraging all the tools and capabilities out there. So if you guys have information or suggestions, happy to engage with you guys to do that. And finally, we will create a website

where we are going to post all of the documents and the working documents, so that people can access it and use it, and contribute to the overall concept. That's really all I had. I want to open it up to question. Brian, Budge,

Do you guys have any comments or questions that you would like to add or clarifications.

So let's…I'm going to ask you to hold on Brian and Budge

Because we do have quite a few questions that have come in. So first of all, thank you. And we're now going to start the Q. A. Portion of the session. Just a reminder to everyone. You can use the Zoom Q

A feature, which several of you have, or you can press the raise your hand, button and I will, because we have gotten several questions in, I will add the note

that we probably won't get a chance to address all of the questions on today's Webinar. What we will do is provide your questions to our presenters,

the ones that we can't answer today on the Webinar, and we will then post answers for those questions along with

the recording of today's Webinar.

So, the first question that we had come in asked,

How does a 911 Agency take advantage of this Certificate program? Can they be voluntarily involved in the testing?

So, so, in a short answer, Yes and no. So, in the preliminary testing phases, Yes, absolutely you guys, But what we want to do is centralize the actual.

So, in all of the pre-activities until we get to the actual physical certification, you guys can be involved. And, whoever that is that sent me the anonymous note. If you don't mind reaching out to Sherri, I'd like to know what you guys did on the Mission Critical push to talk. We're very interested in that.

So, so the answer in the short answer is, Yes. The certification program, however, that has to be done in a very controlled, repeatable manner. So, you guys can participate in all aspects of it, including certification, if you want to go to a certified lab and participate that way.

But we certainly are going to open that up.

Okay, Thank you.

So, the next question is, yes, with NENA i3 architecture and standards include conformance and interoperability testing.

Oh! Okay, Wait. Sorry, we have someone who raised. Sorry, we had someone who raised their hand. So um, Regina, did you want to ask your question?

I apologize. I'm in a very small screen. So, Regina go ahead.

yeah that's okay, I'll ask you the questions and that way I can keep track if someone raises their hand.

Okay, great.

It looks like Regina. You're still muted. So, if you wanted to unmute yourself.

No I don't have a question. I just was wondering if you could make the presentation available after.

Yes, it will be available on 911 dot gov

Sorry. Thank you. Sorry.

That's okay. Thank you.

Just please be advised that as we are, you know, we're sort of building the plane as we're flying it, so some of the deliverables may change, but you know, and also availability of funding right now, and we

believe we have enough funds to finish phase three and actually stand up the program.

But again we're working through the details. So, so Regina. Yeah, I think Sherri's answered your question.

How about we answer like two or three of these, and then I will submit written responses

Right! So the next one. I think you had started to read. They're asking that, NENA i3 architecture and standards already include conformance and interoperability test cases, and are you working closely with NENA.

Absolutely. We think NENA is one of our key program partners in this. I am not going to recreate the wheel. If NENA developed the i3 standard, and they've developed architecture and

other items. Absolutely. We're going to leverage it where we want them to be part of the broader governance team,

you know, technical, as well as program governance. And then there is going to be a government, a government

governance that's only going to be focused on policy questions, and that will be made up of Federal, State, local users and government employees. So we are expecting key folks within NASNA to be part of that government,

governance. Sorry that's, it's kind of a mouthful.

Okay, Thanks. So, um we have time for one more. And this question says, How will public safety digital transformation help agencies achieve successful tested NG911 interoperability?

Okay. So this is a great question.

So with regard to, um, considering,

I think the answer is that if you have a confirmed certification program and a list of â¦ o actual test cases that you're going to do in a lab, you're certainly giving the best opportunity to ensure interoperability in the field.

Now, obviously these programs, these systems are so complex,

and you could fail a test because the router or switch, or it isn't set up correctly. And, so, certainly what our guidance and..and format is going to be is we're going to test it to the best of our ability in the lab. You know, given the trade-offs, right? Now,

we're not going to be able to test as completely or as thoroughly as we want, just because of cost, time and functionality.

But we want to get to, you know high priority items that are confirmed and tested and validated. And then the other component of this is that the test cases and actual activities that we are going to be using,

they're certainly going to be available.

Those test cases are going to be published. So if any operator, user, wants to buy a program, and you you've tested in the lab, and you want to take some of those test cases and run them in the field to verify

that the lab and the field conditions are,

are, you know, they're faithfully represented, then you can certainly do that.

So I kind of have to break up at this point. I apologize, but I've got a conflict.

but, Sherri, if you can get me all the questions. I will take my best to answer it. But obviously I will rely heavily on Budge and Brian to make sure I'm not going off the reservation on some of these answers.

Yes, thank you. We will. And thank you again for joining us and for being willing to share your presentation.

Yeah, you know, I really appreciate it. Thank you all. By the way, I want to thank all of you guys for what you do. You know, vendors, users, 911 operators. By the way, we're also doing some other great research on AI machine learning for

for telecommunicators to reduce their burden. by automating processing of video and some other things. If you guys want to learn more about that please do reach out to Sherri. And, she'll, she'll drop me a note and we'll send you links or information.

Thank you, Sherri, for setting this up. And Brian and Budge, thank you for your guidance.

All right with that I am now going to ask Brian to introduce our next speaker Budge Currier.

Thanks, Sherri, thanks Sridhar it was great presentation. Our next speaker is Budge Currier, since twenty eleven Budge has served with the

California Office of Emergency Services or CalOES. And in his current role Budge is responsible for the 911 system that supports the 438 PSAPs with over 27 million 911 calls per year in California.

He manages the Emergency Communications Division and serves as California's statewide interoperability coordinator, or SWIC, to provide the communications planning, coordination, and response. Budge also serves as President of the National Association of State 911 Administrators or NASNA.

And, without further ado. I'll turn it over to you Budge.

Hey, thank you, Brian. I appreciate that.

So feel free to type your questions in the chat window. I'll try and address them as I roll along. I've got that window open. So, if you go to the next slide. I'm going to give kind of an overview of, um not next gen 911. I've given this a couple of times, and I think it's helpful to kind of frame the conversation. I'll very quickly go through our system, and then get into some nuts and bolts about component testing and end to end testing,

and some of the lessons that we've learned here. And then really to address some of the comments in the chat window. You know, CAD to CAD and data sharing, based on the EIDO and the EIDO conveyance. So that's kind of a high-level summary of where we're headed. If you'll go to the next slide.

This is, obviously there's a bunch of acronyms. I'm not going to read all these for you, but each of these pieces and parts

are contribute to the call flow with next gen 911. So I put this slide in here just so you can refer to it, and on the next slide we're going to go through a use case, if you go to that.

And on this one Sherri, there's a ton of clicks. So, as I say, Yeah, there you go. So the first thing that happens is you make a 911 call, hit the next, it goes into the ESRP, which is the routing engine. It goes

down to the carrier-based list, which returns location information. Most of the carriers do not have these built yet, so each of the providers has to build a location database. So it goes and gets the routing at the civic address

or the XY. From that location database, it comes back next to the ESRP. At this point we now know the location, either civic, or XY, so from the ESRP it makes a query. Next

hit it two more times. It goes out to the ECRF. Which this is where your PSAP boundaries are. So these are your shape files that define the PSAP boundary. So it's literally taking that boundary plot in the X Y or the civic inside that boundary. And now we know where this call should go geospatially. So the next thing we do

we send that down to the policy routing function. This contains information about what to do if the PSAP is not available, or if all telecommunicators are on a call and it's not available.

Once you know the policy, you send the call down to the PSAP with all the information, location, and everything, right in the header of the message. And if you hit next, text to 911 uses the exact same process, which is different, than the way that it works today.

And in order to keep all this maintained on the next slide, Ah hit next. there's a service order input process that is maintained by the carriers to make sure that the location database is kept current. For carriers that have a list of location information server, this step is not needed.

Now. All of this to say, When the media payload arrives at the PSAP, it's got the header, the phone number, the location, the URI, which is the uniform resource indicator, or uniform resource locator.

All of that is in the packet that goes to the PSAP. So this is what we're testing. And, it's not trivial, because each piece and part of this

could be a component level that needs to be tested. Say, an ESRP or a policy function, or an ECRF or a list,

and as well end-to-end testing needs to be accommodated.

Where you would send a call all the way in from the left side of the Graphic all the way to the far right side, where it's being answered by the call handling equipment that's located at the PSAP.

So if you go to the next slide,

This is an overview of what we've done in California. I'm: certainly not going to read this slide to you, but we've got a very complex network here. There's four different

Providers, Atos, Synergem, NGA 911, and Lumen, and each of them is interoperable with one another full end to end interoperability.

In other words, an entire system could go offline, and the other one would pick up the load.

The entire system is using IPv6 with a software-defined wide area network attached to every PSAP. And it's i3 compliant, using geospatial routing and location is delivered via a SIP, which is session initiated protocol.

We've also implemented if you've heard of the PSAP Credentialing Agency, or PCA, that actually implements the private key infrastructure. We've done that. So we've done

a tremendous amount of work in California. The system is up and operational we're transitioning from legacy to next gen now. But along this journey we've tested a lot of things and learned a lot of lessons that we've been in communication with um Sridhar and others about this.

So the question came in, How does our lab connect to a carrier list to obtain location specifically if it's operated by a third party like Intrado or Comtech. So we actually have

connected up to both Verizon and T-Mobile to test their lists, services.

And the way we do that is, we connect them in to our test environment over circuits, and then we receive that location either by value or by reference. Most of them are doing it by reference, and then we dereference that, and go back out and pull it in the location, just like the previous diagram was showing.

Okay, next slide.

This is just a graphic showing you how we broke our State up. So basically the northern part of our State is managed by Synergem, the Central and L. A. Regions are by NGA, and the South is Lumen, and then Atos is connected to every single PSAP in the State.

And we've tested Failover in an i3 environment where, if any one of these goes down, the region, say Synergem goes down, Atos picks up the load. Or the central region goes down, Atos could pick it up. Or Lumen goes down, Atos could pick it up. Where NGA goes down in L. A. county, Atos could up that load.

And we've tested this full end-to-end interoperability

in our lab, and at PSAPs out in the field. It's part of our fail-over testing process. We've written scripts all the way down from, we start an ingress into aggregation, and then we test it all the way to the distant end, where it's actually delivered

to the call handling equipment, and answered there.

On the next slide. I think it probably provides a little bit better graphics because you get kind of a sense on this slide.

The PSAPs perspective. So you can kind of see the top part in blue. That's the Atos network. The bottom part in red is the region provider. Every PSAP has a region and a..

and Atos connected. What we've got is we've got, you see these, there's two lines kind of running parallel to each other. Those are two fixed fiber connections

from two different providers. This robust LTE solution. We're actually using a product by a company called the Dejero. That's a multi-sim active active solution. We put all that into an SD-WAN. So from the PSAPs Perspective there's

logically one connection back in the region. But we've got multiple connections that feed into that SD-WAN. And then we do the same thing for Atos with the additional connectivity across the State microwave.

You can see on the bottom there, our legacy network has an average of about forty thousand minutes of outage every month, and that's averaged over the last twelve months. Since November of last year, we've had this, this network active and monitored into…we're getting close to three hundred PSAPs now

zero seconds of downtime

in that timeframe. Matter of fact, yesterday we had an outage in California. It affected 37 PSAPs. I'm Sorry, 27 PSAPs.

Had Next Gen been active, those PSAPs would have all stayed online. So this network of topology works. We've tested the failover testing from aggregation, failing over to different next Gen Providers.

When the core fails, failing over to neighboring core, and then, when any of the individual circuits goes down, we test that and fail over. And, we've tested the interoperability with a number of call handling solutions.

So question here, since California has already implemented their own testing scripts, Will you use anything from DHS S&T? Yeah, we're actually working in close partnership with them. I've got a couple of members of my team that are on the working group. We're contributing by providing our test scripts to them that they can then write the back end processes for, to test that,

and once the testing process is complete, we'll just have our next gen vendors go through that and get certified. And we're pretty confident that we'll learn some things that we probably didn't learn on our own.

Question came in: Who pays to the connectivity, to Intrado and Comtech? We pay for that in our system, up to a certain point. Obviously, if Comtech's meet point to us they pay for it. But for them back in the network, we pay for that.

Next question, How do carriers deliver test calls made from certain devices to the lab as opposed to the PSAP? That's a great question there. So one challenge you run into is that the only way to really test the carrier network is to dial 911, and the last thing you want is for a 911

call that's dialed to be sent to a lab. So we've gotten a couple of test devices that are appropriately labeled that will terminate in our lab, and we're using that for testing, is how we did that. Um, let's see.

What question am I on?

Yeah, Budge, let's go ahead. Let's go ahead through the presentation, and then we'll circle back and catch some questions.

Okay, fine. Next slide, please.

I only have a couple more and we'll be done.

So hopefully I can leave some time. So this graphic here is supposed to help understand the various components that need to be tested individually.

And, then the end-to-end testing that needs to be tested in order to validate that you've got true to end-to-end interoperability. So the blue line would be simulating a call coming in to a Next Gen Core Service provider through their ESInet all the way through to PSAP A.

And then you realize, oh, wait! That call needs to be transferred to PSAP B. So that's this red line that comes down through to PSAP B. In order for that to work,

both ESInets need to have a meet point. Both Next Gen Core Services need to be able to communicate with one another

And absent, you know the Forest Guide, you're going to need the Forest Guide in place. There's a way to solve that without the Forest Guide fully implemented, which we've done. And then

it arrives in at PSAP B. You've got to have the call handling equipment at PSAP A able to interact with Next Gen Core Services on the top

with Next Gen Course Services on the bottom, and then the different call handling equipment down at PSAP B.

And so that's really the level of testing that we're doing and the starting point of where this is. So basically, starting at the ingress of the network all the way through in order to deliver to the call handling equipment. Now,

long-term, we've talked about the conformance and end-to-end testing actually supporting the details of the interaction between the handset and the network provider and the aggregation of the NGCS. That's also something that will be addressed in the process.

And then, if you hit the next slide.

This is some of the things that we've learned. Now a lot of this is way down in the weeds. But you know, obviously these networks are connected using BGP. You heard Sridhar talk about how

one little router misconfiguration will essentially make it so you can't pass the testing. So this pairing of networks is really important. The routing becomes very complicated, and you've got to have proper,

you know, network engineers working on this.

Inevitably, some networks are going to be IP version six others are probably going to be IPv4, and we're learning that not everybody is up to speed on IPv6 in a production environment.

The transport layer Security and PKI, Private key infrastructure, those things are really challenging to get right, and they make it difficult for troubleshooting. You need a unique IP address to that that's public facing in order to support a carrier-based location information service. In other words,

for my CPE, when I go dereference that location, I need a unique location to turn that back to.

And then, the standard has different methods of transfers, and quite frankly, other things in the standard where both are correct. If Company A is using one method and Company B is using the other method, they're not going to be able to pass the end to end

interoperability testing, even though they are compliant with the standard. Um, the LDB is quite messy. So, um it's a challenge for you that you have to come across. And really this is just so important to go through this process.

The last slide that I have. I think it's the last one, is kind of walking through an example of where we're going next. So like I said, all the way from the aggregation to the delivery and processing at call handling equipment, or CPE, is the starting point.

But really the next step is testing EIDO and the interface between CPE and CAD across EIDO. And then, if you hit the next slide.

Actually, from CAD to CAD, using EIDO conveyance. So CPE interoperability takes the audio and a call from the location from CPE to CPE, whereas CAD takes the actual whole entire emergency data object

and moves it from one PSAP to another.

And that really would be you know the follow-on step to this interoperability, testing. Let's lay the framework, get the base tested, validated, and in place, and then move on from there.

So that's my last slide to kind of give you an overview of where we are. And then I think I see where we are on the questions, So

Yeah, so we're on, we're on, the one Budge, that said, Is there a default (yep) PSAP for each region in the instant of an ALI failure?

Yeah. So Steve, Yes, there is a default PSAP for each region, and technically at that point it's not an ALI failure because we're not using ALI, but I think I understand exactly what you're talking about. We've set up a default for each region, and we've also set up a default statewide.

PSAPs in California made the transition to full NG 911 today. It's a small number. Only five. And the reason for that is, we're working through the final challenges in the exchange with the existing call handling equipment.

So we got five of four hundred and thirty-eight Yes, Donny. We have a lot of work to do. Let's see. Design for OSP. Okay,

So the,

Sorry go ahead

Yeah, no, that's, I was going to prompt you that, the design for OSP.

Yeah. So the OSPs to interface with the two ESInets in a region. What we did is we segmented the traffic for the OSPs as primary and secondary. So in California, Atos is the primary aggregator for voice over IP, and all the small local exchange carriers. The Regions are the primary aggregators for wireless,

and the large local exchange carriers. These are our two legacy LECs that manage our selective routers.

And that way the OSPs know where to direct their traffic. Now we also built in hot standby circuits, and depending on the wireless provider, the capability to switch over to them is a different, slightly different process. But essentially, if the region is not available for wireless,

and the carrier's connection to aggregation is the problem. If aggregation is the problem, we have fell over mechanisms on our side. But if the carrier can't even get to aggregation, we have a mechanism in place for the carrier to direct connect into Atos as a failover mechanism.

And then our experience in having them connect has been very favorable, actually.

General intent to take this beyond i3 testing to CAD, and perhaps FirstNet as well?

So yes, we certainly want to take this beyond just i3 call delivery into CPE. I talked about the CAD and EIDO and the EDIO conveyance. So yeah, we definitely want to do that.

So there's forty three thousand minutes in a month, All right. So good job on your math. What we've done is we've counted up all of the downtime

for the legacy circuits into a PSAP where the PSAP is offline, because the Next Gen 911 network is not available.

That's what that metric means.

All right, and the next one: Do the four hundred plus PSAPs already exchange data? No, they do not. Some do, but most don't. Um, and is the NENA data format and exchange standards going to be used?

Yes, we'll be using EIDO and an EIDO conveyance. We just signed a contract statewide for, we call it data sharing, which is basically a CAD to CAD. You can get the details of that on our website.

Okay. So yeah, So we're running. Yeah, we're running a little short on time, and I know we have several more questions that have come in, Budge.

So we'll do the same thing for you that we did for Sridhar. We will pull the questions down. We'll send them to you in a document so that you can provide written responses.

And I will let everyone know that again, the recording, the PowerPoint presentation, and then those question and answers, will be posted on 911.gov in the very near future.

I want to thank you so much, Budge, for the time today for joining us. And speaking,

this was a very popular topic, and folks had a lot of questions for you.

Well, thank you. So an opportunity. I really appreciate it. Sherri. Thank you. And thank you, Brian, for the, for facilitating this as well.

Yeah, Great session.

So, this concludes today's Webinar, and certainly we appreciate everyone's participation. As I just noted an archive version of the Webinar will be available on 911.gov soon.

Just as ah a point of reference. We will be sending those questions to our seekers, so it will take a little bit of time for them to provide you answers in writing, and once we have those, we'll get all of the information posted to the website.

As a reminder. Our next Webinar is scheduled for November the eighth at noon Eastern time, and we hope that everyone will be able to join us.

Thank you again, and have a great rest of your Tuesday.