UNITED STATES ELECTION ASSISTANCE COMMISSION

TECHNICAL GUIDELINES DEVELOPMENT COMMITTEE
ANNUAL MEETING 2025

Held at

9:05 a.m. EST

Tuesday, January 14, 2025

National Cybersecurity Center of Excellence

97900 Great Seneca Highway

Rockville, Maryland 20850

The following is the transcript of the United States Election Assistance Commission (EAC) 2025 Technical Guidelines Development Committee (TGDC) Annual Meeting held on Tuesday, January 14, 2025, at 9:05 a.m. EST.

***

CHAIRMAN HOVLAND:

I'm Chairman Ben Hovland of the EAC and the Designated Federal Officer for the U.S. Election Assistance Commission. The mic is working, adjusting for that. And so, I'm the Designated Federal Officer for the Technical Guidelines Development Committee, and I'm calling this session to order. I don't have a gavel, but I'll just do a little tap there on the table to get us going.

Just to start off, I'd like to ask everyone in attendance to rise and recite the Pledge of Allegiance.

***

[Chairman Benjamin Hovland led all present in the recitation of the Pledge of Allegiance.]

***

CHAIRMAN HOVLAND:

Thank you. I'll now turn it over to NIST Acting Director for Laboratory Programs, James Kushmerick, for opening remarks. Thank you.

MR. KUSHMERICK:

Well, good morning, everyone. Thank you for being here. As mentioned, I'm Jim Kushmerick. I'm the Acting Associate Director for Laboratory Programs at NIST. In government

agencies, whenever we have a transition of administrations, a little bit of a shuffling goes on, but I'm really happy to be here to represent the NIST Acting Director. Mr. Chuck Romine really wanted to be here, but he's been called downtown for a meeting with the Secretary of Commerce. Even though it's the last days of the administration, there's a lot going on for handoff and transitioning.

But, like I said, I'm honored to serve as the Chairman of the Technical Guidelines Development Committee in accordance with the Help America Vote Act. To be completely honest, until recently, I didn't realize NIST did this --

[Laughter]

MR. KUSHMERICK:

-- or was a partner to help do this to be quite honest. But when I think about NIST -- and you know, or hopefully you're aware, we have many roles. You know, we have technology leadership for critical and emerging technologies. We provide foundational trust for measurements, specifically for commerce and for other areas, and we provide fundamental research to always do that, so this really does fit into our big purpose of enabling trust in science and technology, to enable trust in voting. It kind of fits within that purview. So it makes perfect sense, and Barbara's

briefed me up to understand how we work in this area, so it's great, you know, and it's great to be here.

We're pleased to host you at the NCCOE, the National Cybersecurity Center of Excellence. This is where we bring together experts from industry, government, and academia to tackle some of the biggest cybersecurity challenges, and I know that's one aspect that you all have been working on and that you've been partnering here for voting security.

Today, we will touch base on current program updates from both EAC and NIST, including some exciting new research by NIST on voter trust and confidence. We'll also hear about resources for accessible voting, advances in ESTEP program and some lessons learned on E2EV voting.

On our agenda today, we will first hear from EAC Chair Ben Hovland, followed by Monica Childers, the Alternate Designated Federal Officer for this committee. I was asked to especially give a call out to you, Monica. The NIST folks have really enjoyed working with you. And finally, EAC General Counsel Cam Kelliher will go over the meeting rules, and then we will get to the technical heart of the meeting.

Today's meeting is primarily an information-sharing meeting where we do hope to get insights from the TGDC on current work at the EAC and NIST to guide us in working and moving forward. I

look forward to fruitful discussions and, once again, thank you for your time and dedication to improving our nation's election system.

Unfortunately, I'll have to leave after a little bit of time. Our annual award ceremony is tomorrow at NIST, and we have so many great people, and there's so many awards -- Barbara included, yes --

[Laughter]

MR. KUSHMERICK:

-- and all the NIST people here, not just Barbara, that we --

MS. GUTTMAN:

Well, let them.

MR. KUSHMERICK:

I know, but I'm just saying many people are great, but yes -- that we have to do some planning and rehearsals, and I have to make sure I pronounce people's names right and all that. But when I do leave, I'll be turning over the chair to Ben Hovland to kind of complete today.

So without further ado, let me turn it back to Ben, who will go with his introductory remarks.

CHAIRMAN HOVLAND:

Thank you. Thank you, Mr. Kushmerick, and thank you to NIST for hosting today's meeting once again this year.

For those of you who I haven't had a chance to meet, I am, again, Ben Hovland, Chairman of the EAC and DFO for this committee.

I hope everyone's had a restful holiday season. I don't know that I personally got as much, and still, I know particularly for the election officials, you know, there's never enough time to make up for a presidential election year. But certainly, we appreciate everyone joining us today, especially with all the weather uncertainty. As you can see, particularly for the D.C. area, we've gotten a decent amount of snow recently. My kids were out of school basically all of last week, as I know many others in the area were. But excited about this conversation and continuing the work.

Today, you'll hear more from our EAC Testing and Certification team. We are excited to have had a third 2.0 voting system submitted at the end of December, the VotingWorks VxSuite 4.0. So, again, that is the third system that's been submitted to the 2.0 standard, which to me is really sort of a testament to the work that this committee did now many years ago, but good validation of those efforts and to see that continuing to move forward.

We're also excited to share updates over the past year from two of our newer technology programs, the Election Supporting

Technology Evaluation Program, or ESTEP, and our Field Services Program.

And I would like to note that with Jon Panek transitioning into his new role at the EAC, I want to recognize and acknowledge two members of our team, senior subject matter expert Monica Childers, who took over the TGDC's Alternative Designated Federal Officer, which is why you get emails from her and saves me a whole lot of time, so I am very appreciative of that. And then Brooke Watters, who you'll hear from later, who's the acting Testing and Certification Director.

I also want to take a moment to recognize the hard work of election officials and workers that ensured the elections across the country ran smoothly in 2024, some of whom are both on the committee and then also here as well. And with the 2024 presidential election now behind us, we're looking forward to fruitful discussions today to guide the ongoing work. In elections, the work never stops. And so, again, many important things to talk about, talking about the VVSG, looking forward to how we continue to build and ensure functionality, accessibility, and security of our systems.

And with that, I will turn it over to Monica Childers for a roll call. Thank you.

MS. CHILDERS:

Thank you. When I call your name, please indicate if you are here.

***

[Ms. Childers called the roll.]

***

MS. CHILDERS:

Thank you so much. At this point, we don't have a quorum, so we won't be proceeding with any votes today.

Before I turn it back over to the DFO, I would also like to do a little bit of housekeeping. If you do have cell phones with you, please do turn those phones to silent for the duration of the meeting. That will help us and help our capture to hear as we go forward.

These mics on the table are floating mics for our members who will be able to join us and speak today. If you need to turn a mic on, please push the "on" button once. Do not hold it in while you're talking. That will power cycle the mic, and you will no longer be audible.

I also have one- and five-minute warning cards over here just to help us keep on time. If you're up presenting and you see me hold those up, that's the amount of time you have left in your designated presentation slot.

And finally, all of today's proceedings will be available to the public after the meeting in the form of a transcript. If you would like to receive a transcript, please just let us know.

And with that, I'll turn it back over to the DFO. Thank you.

CHAIRMAN HOVLAND:

Thank you. Camden, I don't know if you want any rules, or I think the summary of the lack of quorum means that basically this is technically an information session, but the big difference is we'll have to pause the adoption of the minutes until next time, as that was really the big vote piece here, but otherwise, essentially proceeding as scheduled.

And so did I cover it? Excellent.

I'd also like to acknowledge my colleagues, Vice Chair Palmer and Commissioner Hicks, who are here as well.

But with that, I think we'll jump right into it, and I'd like to welcome Brooke Watters up, the acting EAC Testing and Certification Director, to provide an update on the Testing and Certification Program.

MS. WATTERS:

Good morning, everyone. So my name is Brooke Watters. I am the acting Testing and Certification Director here at the EAC, and I'll just be going over some program updates, mostly focusing on what we've done in 2024.

Before I get to my updates -- and some of them I will make brief because there's a lot of content here. I just wanted to say thank you. Thank you to NIST for hosting this at their facility. Thank you to the Chair, the DFO, the ADFO, all of NIST staff and EAC staff for putting this together. Without them, we couldn't do this, as well as the materials that you'll see here today.

And thank you to members. We appreciate your attendance here. This meeting and committee is very valuable to our program.

So this is a little bit of a recap. Chairman Hovland has already covered this. Jon Panek is still in the room. He's still very much part of Testing and Certification, though he's now gone to the acting position of the Chief Election Technology Officer, so he oversees Testing and Certification, and I work very closely with him. And so you're still getting a lot of -- we share the same kind of thoughts and whatnot here, so talking with me is still like talking with him. And I have been doing the acting director role since August.

Just a quick share, we are looking to hire, and we're in the process, I believe, of onboarding another election technology specialist for our Testing and Certification team, which actually brings our team, when including Field Services, to a size of 10. This is significant in the sense that we have resources, right? I think at one point we were down to a team of two people, not that

long ago, and now we have a team of 10, not including the ESTEP team.

So the big thing I'd like to start with is the voting system campaigns that our program has seen recently. Here at the top, we have VVSG 1.0, and these are the last of their kind. All three of these systems got their applications in before the deadline of November 16th, 2023, in the lifecycle policy, allowing them to have full maintenance modifications. Campaigns go through Testing and Certification. Anything beyond this that's submitted to 1.0 must adhere to the limited maintenance exceptions that's outlined in that lifecycle policy. These made it in before that deadline, and these are the ones that are just going to make it through.

So, very quickly, at the top, last year we saw ES&S's EVS 6.5.0.0 receive certification. We have Dominion's D-Suite 520, which currently is in the initial decision to certify. And we have Clear Ballot's ClearVote 2.5, which is still under test. For VVSG 2.0, we do have three systems under test, which is very exciting. We have Smartmatic's VSR1 2.1. We have Hart Verity Vanguard's 1.0. And, more recently, we have VotingWorks' Vx 4.0.

Following the schedules laid out by their respective laboratories, we expect to see Smartmatic reach completion in the fall of this year, 2025, Hart Verity Vanguard in the spring, and VotingWorks, their application has actually just been recently

reviewed and approved over the weekend. This will be updated on our website later today, so we don't have a schedule for them, and they're all in slightly different stages. And this is barring that there's no additional hiccups, but the schedules are pretty robust and built by the labs to anticipate for some of that.

I do apologize because some of the text on this screen is a little bit small, but effectively, the minor change orders that we saw are all subject to the limited maintenance exceptions we have in the lifecycle policy. This means that we're no longer receiving minor change orders for just quality-of-life updates to systems that are legacy and currently out there. We have to have them meet either a security update, a bug fix, a jurisdictional rule change, an end-of-life cost replacement, or item #5, which we're not seeing until we've gotten the Component Pilot Testing Program or some other pieces up off the floor is items individually tested to the newer standard, VVSG 2.0, while the rest of the system comes in for certification under the legacy standard.

So we've actually had to turn away at least two minor change orders because they did not meet that. We saw a total of 26, most of these being end-of-life COTS replacements listed under hardware. But we did see some software updates, mostly some configuration files, and some technical data package changes as well. The graph on your right is outlining how many there are. The

graph on the left, we are able to track our turnaround time. Once items are given to us by the labs and the manufacturers and their due diligence has been done, how quickly are we at the EAC able to turn around these items and get them back out for approval so they can be deployed? This is important for things like security fixes or bug fixes, making sure that we're not holding up this process.

And, on average, regardless of the type of change we're seeing, it's about a 2.5-day turnaround. This particular metric actually does include weekends. It doesn't do business days only, and so I think it's actually even a little bit quicker than that. The fastest we've seen is a day turnaround. The longest was six days where we received it on a Friday, so relatively four days. So we're not trying to hold up this process at all.

In 2024, we published three new RFIs, the unique identifiers, unauthorized physical access alerts, logging of physical connections and disconnects. I didn't want to overload this screen with all the information about what requirement that they're related to, so I can brief over those. The unique identifiers talks about adding a unique identifier to the ballot after a voter has cast it and it's no longer in their possession so it cannot be identified by the voters or the public, but it is used for auditing purposes. And it needs to be done after casting at the time of the cast vote record

creation so it is captured in the cast vote record. And this needs to be done for anything that does cast vote record creation, which includes precinct scanners and central account scanners.

For the unauthorized physical access alerts, this question was actually more geared towards the storage of ballots and ballot boxes and asking if a ballot box door that is, you know, not through the optical account scanner, does that need to alert and alarm poll workers when it is open and closed? Ballot boxes aren't typically wired in with technology, and so that's not something that that requirement is intended to do. This requirement is more along the lines of safe compartments for electronic media, USB drives, and other access components of systems such as of the precinct scanner.

A similar question was asked for logging of physical connections and disconnections in regards to opening and closing of a ballot box door. Once again, using the same logic, it's not expected that the opening and closing of a ballot box door, unless you are having to remove part of the device from it, which would be a true disconnect, is going to cause an event log to appear.

So these are all pretty straightforward. They borderline a little bit of implementation design, but with VVSG 2.0, you see those requirements that talk about the voting system must. It does not have that same granular scope of the BMD does this, the

precinct scanner does this. It's a much higher level, so we can understand why we're getting a lot of these types of questions.

More recently, we do have two RFIs that are in queue. If you haven't been to our website recently, we've actually made an update that we are listing these RFIs that are in queue so people can see what we're actively working on. We do not have a result necessarily, but we're getting a lot of the same question from a lot of different parties, and this way, if they would like to add to the question, or if they just want to wait until something comes about, that gives everyone an opportunity to give a little bit more insight on what we're doing.

The two that we have are accessibility features, which the question states, "All voter-facing devices at all voting locations include assistive functionality," should they, and that one's currently drafted and being circulated with experts and discussion.

For preserving software independence, that question asks to clarify the ballot selection area and how to identify this space on a ballot to ensure voting systems are not capable of making undetectable changes to the paper record. This one is in reference to the unique identifier as well, which is something that could potentially go on the ballot after it has been cast by the voter.

Common data format updates, this is not new to the VVSG 2.0, but it is important and key to interop. And the update here is

that we need to make sure that we're seeing consistency when using the common data formats. This is across devices, as well as systems. And to achieve that, we need to have consistent testing between our labs. And, historically, our labs will create their own test methodologies and do testing in their own unique fashion and during their assessment of accreditation, making sure that it's up to that standard. We need to go a little bit further here and ask them to effectively do the same thing.

So we actually came to NIST and asked them for their help with this, and they delivered, working in a harmonious fashion with us, to have a test method and a test tool that we have now as of January 2nd, 2025, given to our labs and requiring them to use it on all systems going forward. This definitely ensures consistency across these systems. And the tool, from what I understand -- I've gotten to play with it a little bit myself -- if you go to this QR code, or I can provide the link after, it's on GitHub, you're available to submit feedback, use it yourself. It's a very fast tool. This is not a heavy lift by either of our labs, just something that we want to ensure is happening.

In addition to that, NIST has drafted a lifecycle policy to go along with the tool, as well as just covering CDFs in general, going over things like versioning, compatibility, updates to CDFs, the methodologies, and the co-evolution with VVSG. This little graphic

here focuses on backwards compatibility, especially when doing minor revisions of CDFs. Going from a 1.0 to a 1.1, everything should be backwards-compatible, so we're just looking to move forward and get better.

Federal information processing standards, or FIPS is a little bit easier to say, FIPS is also seeing an update, and some of you might be familiar with this. They are moving from 140-2 to 140-3 and this has been in our program. VVSG 1.0 calls out that 140-2 level 1 or higher must be used. Because we are seeing a standard and technology update in this field, we are keeping up with it and have a language being updated both in our VVSG, as well as our program manuals. And there's a sunsetting period that NIST is doing that a small excerpt is here on screen. If you go to the QR code or to this link, you will be able to see the full efforts.

But, effectively, the big takeaway here is that, what does that mean for our program? And we outline that FIPS must be current to all new systems. Well, a little bit of the issue there is that we're using -- and apologies because it's on issue -- just that we're using different language. The FIPS CMVP team is using statuses such as active, historic, and revoked, whereas in order to keep up with this technology, we are referring to current FIPS must be used. And what does that mean? Because right now we have 140-2 and 140-3 working together with active systems at the same time.

So to try to bridge that gap a little bit here briefly, for VVSG 2.0 systems, current means active. If you're using a 140-2 or 140-3, there's no distinction here, but it must be an active system. It must have an active status. It cannot have gone historic. Four systems that come back in are legacy systems to VVSG 1.0. Historic is allowed. However, we want to check this on a case-by-case basis to ensure that the security is still being met for these systems.

In the instances where you have a 140-2 cryptographic module that was being used on your VVSG 2.0 system, but it has recently gone historic, you still may have a path forward with working with the Cryptographic Module Validation Program team over at NIST and reviewing what module you're using, why it has gone historic, and if there is a path to validation. So you're not necessarily stuck here, and there is a path forward for this.

So before I pause for a discussion, I did want to go over and just add in the program manual updates that we have as well. So our program manuals are both undergoing redline changes and being updated to version 3.1. These QR codes are current. However, they are for our first draft of redline changes for the Testing and Certification Program Manual and the Voting System Test Lab Program Manual. And the federal registration is actually a comment period that was open and closed in October of November.

This is not the only public comment period that we will be having, so you did not miss it. We are making additional and redline changes, and we'll be posting again here shortly, and we'll be making that public and known. But if you would like to see the comments or the redlines as they currently are, these are the QR codes and can be shared after.

But to help go over what some of these changes are for our Voting System Test Lab Program Manual, effectively, we are updating the language to align with the NIST handbook 150-22. This mostly is updating the core competencies and the subcontracting processes for core and noncore competencies of the labs. This allows for the Chair of the Commission to delegate an agency authority to sign certificates of accreditation, and it includes language from a notice of clarification we have published in 2021 for Voting System Test Lab accreditation reassessment. And getting that language in there, there was a lot of questions around what reassessment looks like and why the certificates look the way they do. And now this is officially going to be a part of our manuals.

For the Testing and Certification Program Manual, we have made some updates to the timeline for reporting anomalies and malfunctions from both the public and the manufacturers from 15 days to 2. There are some additional qualifiers in here, and that's

part of the comments we have received as well as those two days from the occurrence or two days from being notified, and all of that is currently going under review and evaluation. But, effectively, we don't want to sit and wait and get this information way late in the game and be surprised by it ourselves. We're trying to keep up-to-date with what's happening with our fielded systems.

Similarly, we've updated the manufacturer agreements to require the names of their clients and the systems that they have fielded. We are removing the timeline constraints for provisional preelection emergency modification. This does not remove all other items, such as requiring a jurisdictional rule change or sign-off by the jurisdiction. It just simply removes the timeline, which is a little bit constrictive and effectively unable to be used.

We've also made the clarification that penetration testing is done independent from the test readiness review. While this is happening at the same time during the application stage, these are independent procedures, and both are needing to be done before an application can be approved and put into our program.

And, as we've discussed, we're updating the FIPS notation, making it more generic for an easy transition to 140-3 and likely to additional -- I don't foresee a 140-4 coming out anytime soon, but we are preparing for this and wanting to keep up with technologies.

The last piece is we actually have a new chapter, chapter 9 for vulnerability disclosure. And effectively what this is, is we don't necessarily have a policy in place currently for vulnerabilities and what they are in this space. Vulnerabilities are actually currently uncommonly reported. It's very rare when we have vulnerabilities put out into the public space, and as they become more common and more familiar, as these discussions with researchers is coming up, we want to preamble what it is that the EAC is going to do when this occurs.

A vulnerability is different than a nonconformance -- we want to make that distinction -- and that it is a weakness in the information system, security procedures, internal controls of the voting system that can be exploited by a threat source. And so this chapter really just outlines what's the EAC's role. And, effectively, we want manufacturers to take the lead, whereas the EAC may mediate between researchers and manufacturers. It really is up to the manufacturers and the reporter to determine things like severity, the actions that are needed to either mitigate or remediate, coordinate of the fix, and this, again, should not be used to identify VVSG nonconformances.

Effectively, our role is that, once this is fixed and it gets back into our program, we are aware of what's happening, but that is where we really take it on, is during the testing and certification of

these items, whether it's a minor change order or a modification or a new system that's being submitted. But until then, unless we are called for assistance with this mediation, this is really up to the manufacturers and the reporters.

So I know I just threw a lot of information at you very quickly. I do apologize, and I can't go too deep onto any of it, except for now, we have an opportunity for a bit of a discussion, so I will pause if there's any questions on any of these items or any thoughts that you may have.

Yes?

MR. SCHOELLER:

Shane Schoeller with the EAC Board of Advisors. Your last point regarding vulnerabilities, I know she said e-certification only if necessary there at the bottom. What does that look like in terms of if you have a manufacturer that continually does not report a vulnerability? What does the follow-up look like? How do you address that? Because I know we have a lot of people who are interested in security of our election equipment and what takes place. Just a little more information on that might be helpful. Thank you.

MS. WATTERS:

Sure. We actually have vulnerabilities outlined in the VVSG and already have requirements in place for these manufacturers

and these systems on how to address vulnerabilities and ensuring that their systems, you know, any known vulnerabilities are being addressed, mediation, mitigation is being done.

So what this policy is really talking about is when something is found outside of our program in the space of like a reporter and it is being reported, and this is where we may come into place if something is not being addressed or the manufacturer appears to be just not wanting to do anything with it. We may get involved, and at some point, it could qualify as a nonconformance to the VVSG because they should have a management plan in place to address vulnerabilities. This is kind of the starting path to you need to fix your system or technically will be decertified because it is now a nonconformance.

We don't want it to get there. We would like to see everyone doing the appropriate communications and remediation plans and giving that window of opportunity to see it through. It's not an instantaneous you found something, and decertification is on the table. That's not -- yeah.

MR. SCHOELLER:

No, and I just think since it's a public meeting, it's good to have that clarification so that people understand that. Thank you.

MS. WATTERS:

Absolutely. Okay. Well, I will continue on. I do have another piece of this for the VVSG updates. And, again, there is another discussion piece. If any of these questions come up from the first half, please make sure to include them as we go through the additional discussion.

So each and every year, we perform a VVSG annual review, and I want to make a distinction here on what this is because I think it often gets a little bit confused or conflated with when we actually have a draft for a new version in place and it goes out for a public comment period with a set period of time into our FACA boards. Right now, we're actually just reviewing the current VVSG 2.0. There is no new draft in front of anyone. We are simply just gathering feedback from stakeholders and doing that in a variety of manners. This could be from meetings or conferences. This could be from lab evaluations, questions, request for interpretations.

We're bringing all of that together, and we have been for a few years now and actually banking some of this material and have received over 250 comments between 2023 and 2024. And it's a good bit of effort that we put into it to make sure that we're going through this feedback, taking it seriously, working with NIST and our other experts, including the FACA boards, to put together where is the VVSG going, how is it doing, and evaluating it each

and every year, making sure that it's not just becoming stagnant and it's out there, right?

So what we're going to be talking about is the VVSG Annual Review Report, which we have shared with committee members ahead of time, and the recommendation that we have. We are recommending to put forward a minor version update with VVSG 2.0+. It's designed to be a little bit more dynamic, and what I mean by that is to have manageable iterations and keeping up with technology. Some of the updates that I've gone over, including the RFIs, relevant feedback from labs and the CDF versioning, as well as FIPS, right, we're seeing transitions in other parts of related technologies going from 140-2 to 140-3, and we want to make sure that we're keeping up with all of that.

But what is a minor version update? This is not a big scope change. This is not something that we are trying to move the goalposts on anyone here. We understand that there's a development phase that manufacturers are still going through. A common question that I'm sure will come up is that there are no systems currently certified to VVSG 2.0, but with a minor version change, there is no sunsetting period on 2.0. Instead, 2.1 and 2.0 would live side by side and just with a slightly raised bar and a selection of the manufacturer to be able to pick between the two.

So what was in this report that we sent out? Effectively, we've included all of the requests for interpretations. Since the adoption of VVSG 2.0 in 2021, there have been 11 published RFIs. This does not include the two that are in queue or any additional ones that we would expect to get this year. But all of these are in effect. This is not that RFIs and 2.0 are living separately. This is already a part of 2.0. If you're adhering to 2.0, you're also adhering to all 11 of these published RFIs. So, really, the language would just be updated to instead of having 12 different documents that you're reviewing, you would just have the one VVSG 2.1 to review.

Similarly, we've also addressed errata. We've had typography errors, incorrect wording or references. We've actually had a minor formatting issue with the numbering conventions of the requirements naming, and we're looking to fix all that and just get it cleaned up as well.

So, again, none of this actually changes 2.0 rather than just cleaning it up. The change that we would see here is with two additional common data format specifications that have come out that we would like to include. We have the micro common data format specification and the ballot definition common data format specification, and these effectively are in reference to the ballots, the ballot layouts, the ballot information, as well as the machine information on the ballot on where you can find things like timing

marks. So we want to keep up and ensure that we're including the additional common data formats here.

I apologize if it seems I'm going a little fast. My notes are not complete in front of me, but that's effectively the big change that we would see between 2.0 and 2.1. And the potential timeline we see for this happening is, with approval, we would be drafting in the first and second quarter of this year. We don't see this being a heavy lift. This draft would not take months at a time. This is a minor version update.

Once we feel confident with what we have, we would like to post for public comment and get our FACA boards involved with reviewing what this draft looks like. After this feedback, we very much intend to repost for public comment, especially if there's heavy edits to this, and then bring it back to this committee here for a TGDC review.

At that point, when we're feeling pretty confident on this new version, we would like to bring it to our Commissioners for a vote to adopt, and I would like to just simply include that the labs would not need a reassessment. Since this is not a scope change, this is a minor update, our labs would already be able to start testing to 2.1 immediately.

I definitely feel like I'm moving a little bit fast, but we are open for another discussion on any of these topic items.

CHAIRMAN HOVLAND:

I'll start off here because this is an area we'd really love some feedback on. I think one of the things, when I think about this issue area, it really is sort of a transition of time and how this program has been working and how we want it to work. For those of you who have been along this ride for a while or many of you longer than me, you know, which is now, shockingly, six years since Don and I joined. I don't know where that went.

But, you know, thinking back to the 2.0 conversations and what we were hearing about sort of stagnation in the program, you know, I think that a lot of what Brooke has talked about and this are part of that maturing of the program. But we also want to be cognizant of the fact of what that means for the market, what that means for jurisdictions, what that means for state codes that may have adopted HAVA in a very specific way.

And so we want to think through all of those things, but also -- and so it is weird to be talking about a 2.1 in some ways before there's a 2.0 system certified. But, as you all know, and as Brooke laid out there, the HAVA process is not fast, and we're aware of that. And so in order to keep that ball rolling, to avoid that stagnation that we may have seen in the past, you know, it's important to think through that. But some of the feedback we would love to hear is, you know, is now the right time to start that

process? I think, as Brooke highlighted, there are a few minor but important updates that would make sense. You know, I think it's important to distinguish that a 2.1, as it relates to 2.0, is much different than 1.1 as it related to 1.0. You know, those are, what I would say, very different eras of the VVSG. And this is not sort of that whole scale or pretty significant change.

So I just want to put that out there. I don't know if people have thoughts, but, again, we know that it's important to keep this moving. We know that it's important to avoid some of the historic stagnation we've seen. And we know that one of the real challenges of 2.0 was the lift of all of those years of technological advancement, and so having these iterations gives us more time to address specific issues as they come up, you know, and really invest, I think, some of the conversation later, in my opinion, like on E2E. I'm looking forward to that. But, you know, that might have been a conversation we would have had years ago if we weren't doing so many other things in the 2.0 move.

So I know that was a lot, but I'm trying to stall out for Brooke here and give you all plenty of time to think about any questions you may have. So certainly turn over the floor to anyone that has a question.

MS. GOLDEN:

I think this is appropriate to the discussion. I'm not sure, but I believe there's still references to section 508 in the discussion part about complying with WCAG 2.0 for general ICT accessibility. Given the fact that Justice promulgated rules specifically under the ADA that apply to state and local government for ICT accessibility, I would really, really strongly recommend that all of that language be changed to reference ADA because, as far as I know, all the voting jurisdictions are state and local entities and are subject to that. I just think it's disingenuous to reference 508 that only applies to federal agencies when there's an actual legal obligation on the part of all these voting jurisdictions to comply with that under the ADA.

And I think it's just really important, not just in VVSG, but especially in the extra stuff, the voter registration databases, the e-pollbooks, all of that stuff, there is now a legal obligation, and I think it's helpful for voting jurisdictions to understand that because [inaudible].

I think I probably just turned it off because it off because it was sitting on my hand. Sorry. Anyway, that's fine.

MALE SPEAKER:

They're all flashing red.

MALE SPEAKER:

There you go.

MS. GOLDEN:

All right. Turn it this way. It's just changing that reference. And I think you've just pulled the language out of the VVSG into all of the other voluntary, you know, secondary equipment things, so it just needs to be changed across the whole spectrum so that it's clearly referencing the legal mandate on state and local governments.

MS. WATTERS:

That's great. Thank you. That's definitely -- this type of feedback is exactly what we're looking for to add in, so I very much appreciate that.

Something I did want to add to what Commissioner Hovland was saying was that, with this update, we are still trying to find the line of what the change is, knowing that we don't want to alter the scope too grand. We do have a lot of comments that we've banked to go to a 3.0 potentially at some point, but this is not the time. Some of these scopes are a bigger change deal. So to avoid scope creeping, I definitely want some input like this, as well as anyone else has. Where is this line on how much are we changing? We've got a subtle change here to really clean up the document and add in new common data formats. This is an opportunity for some other things to work their way in, but we need to define where this line is, right?

MR. CASKEY:

Brian Caskey representing NASED. So what will be the process if you have a system go through and be certified at 2.0 and then 2.1 comes out? Because, noticing the calendar, the timeline is 2026, which just happens to be the next presidential election, so there will be people that, if there's a 2.1 out there, will misunderstand that and be highly critical of people like me who aren't using machines that are the 2.1. And what will the impact on the vendors be? If there's functionally no difference, how quickly can you get a system that was certified at 2.0 to be certified at 2.1?

MS. WATTERS:

So, just briefly, both 2.0 and 2.1 will be the most current and updated standards to be tested to, so this is not like a legacy system where we're seeing 1.0 systems have gone legacy, and 2.0 is considered the current, which often is reflected in statutes, right?

But, to your point, one of our vendors, who is currently under 2.0, if they're able to meet these additional standards that are coming in, it would not be a heavy lift to come in as a modification. It's just these handful of requirements that are changing, but it's really up to the manufacturer to do that. They're really just adding in some common data formats. Effectively, I don't imagine that this would take very long. It really relies on the bandwidth of the manufacturer and the labs.

But we can definitely help with drafting the language or kind of understanding where these questions are coming from and how they're being shown up because these are the current systems. 2.0 is still very much valid for anywhere in use. I'm not sure if this is answering your question or if you'd like to clarify further.

[No response]

MS. WATTERS:

Okay.

MS. SAUNDERS:

Mary Saunders, with American National Standards Institute. I think you mentioned in your comments that you also would be looking with the Board of Advisors at state and local, you know, requirements and into regulation or into law, if some are more specific than others. And that, I think, is an important point. I don't know that any legislation specifically references VVSG 1.0 or has that level of specificity, but that's an important gap to look at. I'll give you the building code example because there's a model building code that applies voluntarily across the United States, but it has to be adopted by state and local jurisdictions. And many states are several additions behind in terms of what's required, so that would be an important issue to look at.

On a positive note, I would say that I think it's really important in this technology area to keep up with technological

developments and to be flexible, to reflect the latest for trust purposes, also for relevance purposes. But, you know, just keeping in mind the equipment refresh rate at the state and local level, as well as this possible gap in legislation.

MS. WATTERS:

Great. Thank you.

MR. SCHOELLER:

Shane Schoeller, Board of Advisors. First of all, I appreciate the reference to the building codes because I worked with the Home Builders Association of Greater Springfield for a long time. I will say the one comment that I wanted to make regarding the accessibility standards is perfect. You can create the standard, but if you don't have the funding -- and that was one of the issues with local entities is that oftentimes for builders to be able to build to the code, it can often outprice the housing market. And I think that if we're going to look at increasing standards, one of the things we have to be very conscious about is, do we have the funding for the local entities, especially the smaller jurisdictions, to be able to purchase what's being put forth.

And then, secondly, are the manufacturers actually asking for some of these updates in 2.1? Are they looking and saying that we're already outdated with 2.0, or is this just coming directly from the EAC and NIST itself?

MS. WATTERS:

So this report, the first people who have actually really gotten to see this is this committee. This hasn't really been socialized out beyond this. But the manufacturers, they're some of the ones who are asking these questions for the request for interpretations, and so they're looking for some additional clarity here as well.

CHAIRMAN HOVLAND:

I'd just add a couple quick things to baseline for folks as well that I think are useful. The timeline that Brooke put up is probably best-case scenario. But, again, because of the lead times of HAVA, for a trip down memory lane, this board makes a recommendation to the executive director for any change of the VVSG. The executive director of the EAC then sends that to the Standards Board and Board of Advisors for comment. We then have to have a public comment, and we have to have a public hearing before the Commissioners could vote. So the earliest this process could get kicked off by this body would be its next meeting, which is probably roughly a year from now.

And, Brian, to your concern, if by the time we got through the back half of that process, you know, we were squarely in the midterm cycle, you know, I think we would be conscious and aware of that. But I sort of raised that just to know, you know, again, as I

mentioned earlier, in some ways I think it's hard to think about this now where we are vis-à-vis 2.0, but we're talking about this now so that we could be in this position two years from now because that is what the process looks like. Thank you.

MS. GOLDEN:

Yeah, I was just going to say that helps the timeline discussion because, to me, it almost seemed like you'd want to split apart the changes that are non-substantive from the ones that are because then, if you only had the RFI clarifications and all of that in 2.1, you could literally say anybody that's 2.0 is also 2.1, be done with it, and then you avoid that problem of it's not the most current level, et cetera, but it just depends on timing. But I was just going to say, you know, I would almost suggest, then, save your substantive changes for 2.2 or something and do those in another cycle.

And I will clarify changing over to an ADA reference for state and local governments, it's still the WCAG 2.1. The standard, the substance of it is not changing at all in the VVSG or any of your other things. WCAG 2.1 is the technical standard. It's just the legal reference to why you're doing this other than the VVSG. And in this case, it's the fact that now there is something under the ADA, and those rules are also WCAG 2.0, so it's not changing anything of substance at all.

CHAIRMAN HOVLAND:

A question I'd like to pose, sort of, Diane, to that point, you know, part of what I think the challenge of this moment or thinking about this is we've obviously been in an environment with the heightened attention to voting systems. We've certainly seen our fair share of confusion about what the standards mean, what is and isn't current, et cetera. And so because this would be, in many ways, a new way of thinking about system standards, you know, I'd like to throw out there, would doing sort of even more of these -- to your point, if we did a, if we did a scaled down 2.1 that was quickly followed by a 2.2, I guess would that help to normalize this, where this is just a regular process? Because it hasn't historically been, but it does need to be going forward. But also knowing that the, sort of, you know, certainly the broader voting public and many people in the election administration community, you know, are not accustomed to that kind of versioning. So I just wanted to sort of throw that out there for conversation as well.

MR. SKOGLUND:

Kevin Skoglund, representing IEEE. So I'm thrilled that we're doing what I call semantic versioning, this idea of major, minor patch versioning. Typically in the software industry, the way that works is the patch version is really insignificant changes. It would be like the errata, for example, maybe the RFIs. It's things

that really they don't have a significant impact, but it is a change, so we know a change has been made.

Then there's the minor ones, and minor tends to be changes that affect only -- they may be breaking in some small ways, but they're not large breaking changes, right? So there's definitely feature improvements, there's enhancements, and that kind of is what that minor patch, you know, minor version indicates.

And then major, like VVSG 3.0, would be large breaking changes, potentially new hardware. And I think it makes sense to kind of follow that. I would like us to see the lifecycle put out more changes, especially patch changes. I don't see any reason, like the errata, for example, couldn't have gone out the door already.

But I think rather than sort of decide that 2.1 has a quick burst and 2.2 is more substantive, I don't think that's quite the way it's intended to work. I think it's more that you would put out one version 2.1 when you have a large set of changes that are significant but not breaking of the overall system.

MS. WATTERS:

Thank you. And the errata has been posted. However, it did not, as per our lifecycle policy, constitute even a minor version update. It's on our website, though. You can see what was changed. But that's good to know. Semantic versioning is not a terminology that I'm familiar with, so thank you.

All right. If there's nothing else, do I hand it back to the ADFO? To the DFO?

CHAIRMAN HOVLAND:

Well, thank you, Brooke. Let's see. We are a little ahead of schedule. One thing I would like to just again sort of comment about for those of you who are longtime viewers of this committee or of the Testing and Certification Program, I think Brooke's update on the program is really a testament to the hard work of the Testing and Certification team that we're very appreciative of, but also of the agency as a whole's commitment to this area. Again, I feel like, at least in in my tenure, this is a very different conversation than one we had a few years ago, and so really, you know, thankful for my colleagues' commitment to this area and to the team's work at the agency. So, again, thank you, Brooke for that update.

A couple other quick updates, we are ahead of time. We are going to have a break momentarily, but for those members of the TGDC, we're also going to take a photo during this break. And so after I stop talking, if you all would join me up here at the stage, we can knock out the annual photo, and then we will have a 15-minute break, which we're a little ahead of schedule, unless there's anything that Monica has to add that I've missed. Maybe let's call it a 20 so the photo doesn't take away from people's break and back at 10:20.

MS. CHILDERS:

That works. For reference, the restrooms are out these doors to your left and then an immediate right, and they're down the hall. There are signs. Thank you.

[Recess 10:02 – 10:20am]

MS. GUTTMAN:

Brooke, that was an awesome presentation, and I wanted to point out that it shows the close working relationship we're having with the EAC, which I just think is very exciting, that we're really partnering together on some of these things. And you'll see that in some of our presentations, that we're building on work that each other are doing.

So for those of you who aren't familiar, I'm going to start with -- this is actually the same slide I used last year because, truth be told, our role has not changed this past year. So NIST has a couple roles under the under the Help America Vote Act and also roles we have just as part of our general authority to help with science and technology, as Jim mentioned this morning.

So we chair the TGDC. We will find someone to chair it. We're a little light on the management right now, but Jim was actually really excited. He really enjoyed the presentations, and he enjoyed learning about voting and how it fits into the general NIST portfolio.

NIST also accredits labs, which Brooke mentioned. That's not being covered in this presentation. This is only covering our research portfolio.

We helped write the VVSG. It's already written, but we'll help with VVSG either 2.01 or 2.1, whatever it's called. We've been helping, Paul and Brooke taking the lead there.

We've also been providing implementation and auxiliary material to help people implement the VVSG, and we also research voting programs because one day there will be a 3.0. It's going to be exciting. It's not around the corner. People, do not worry. But just as Ben explained, it takes a long time just to make the standard. It also takes a long time to research in order to have material to make a standard. So we also need to be researching next-generation voting systems now.

And also an important role of ours to partner with both the EAC and with CISA so those of us in the federal space are working together to help the election community.

So we divide our work at NIST into three big buckets of research. We have accessibility and human factors, security and assurance, and interoperability. And, as I mentioned before, we sort of tried to look at 2.0 and how to help make 2.0 either come into existence or improve it. And then we're also looking at beyond 2.0, what's in the next generation.

So in accessibility and human factors, we put out two new contractor reports this year. I have a whole chart with them all next. And we started a big research effort in voter trust and confidence, which you're going to get a whole briefing on, so I'm not going to really say anything about it because you see Shanee and Kristen waiting in the wings.

And we have two more guides coming out reasonably shortly on usable audio and legibility of summary-style printed ballots. Those will be coming out soon.

And here's our whole list of stuff we have in accessibility and human factors. I think it's actually really pretty impressively a long list. I see Sharon and Whitney, who were both major contributors to this to help people build the systems to be as usable and accessible as we know how today.

And then we'll be having our next work, the research, which you're going to hear about, so this is just a slide to make sure I remember to tell you that.

In security, we finalized CSF, that's the computer security framework, which is a sort of big deal NIST put out that helps people sort of take a reasonably holistic view of their security, and then people build profiles according to various domains. So we have one on election infrastructure that's been finalized.

We had to draft an implementation guide on multifactor authentication, which is kind of a sticky problem for voting because most multifactor authentications you're familiar with use the internet, and voting systems don't use the internet. It makes the problem a little bit harder for them, and we're thinking that's going to be finalized pretty soon.

And we're also developing some security testing tools. Brooke mentioned that we developed some interoperability testing tools for the CDFs that we then gave to the EAC to incorporate into their program. We're also working at looking at some security tools.

Our upcoming publications, in addition to finalizing the multifactor authentication guide, we're looking at some additional implementation guidance for VVSG. We're working on another cybersecurity profile for voter registration, and we're looking at security and threat analysis reports for election-supporting technologies. And Jay is going to talk about the Election-Supporting Technology Program soon, and we share this information with Jay.

Interoperability, this was a big year for interoperability folks, like, wow. So we put out an implementation guide for the common data formats, which is up there, and we got the test material, which the EAC has incorporated. And, as you can see, we've been working with the EAC on the lifecycle, which is basically going to

promise, if a minor update will have backwards compatibility, major updates will not, the sort of standard in the field, but to make sure, as vendors build to these products, they put a lot of effort into building to these products. They need that kind of assurance that we're not going to rip the rug out from under them midcycle. That wouldn't make them happy, and it wouldn't make our customers in the election world happy.

And this is where to find NIST's work. We have a website, and we have an email.

And with that, I'm going to turn it over to Kristen and Shanee for this work on voter trust and confidence, unless anyone has any quick questions.

[No response]

MS. GUTTMAN:

No? Going, going, gone.

Kristen and Shanee, the floor is yours.

MS. GREENE:

Awesome. All right. Can you hear me in the back? Yeah? Great. My name is Kristen Greene. I'll be presenting with my colleague Shanee Dawkins, perspectives on end-to-end verifiable voting systems, or E2EV, results from interviews with election experts. And I know this crowd is very familiar with the term E2EV, but I will provide a formal definition later in the talk, right before we

get to the results. And also, I know sometimes we hear E2E sometimes E2EV. For specificity and completeness, we will say E2EV in this talk.

All right. Just the standard NIST disclaimer, not promoting or endorsing any products.

So although Shanee and I are the ones presenting today, this research was conducted by a much larger multidisciplinary team. I'll acknowledge each researcher individually, but, broadly speaking, we had an accessibility and human factors team and then a cybersecurity team of SMEs, or subject matter experts. On the accessibility and human factors team, myself, Kristen Greene, cognitive scientist; Shanee Dawkins, computer scientist; Julie Haney, human-centered cybersecurity expert; Mary Theofanos, computer scientist; Jody Jacobs, computer scientist. Now all of us are from NIST.

We also brought in two external qualitative methodologists, Sandra Spickard Prettyman and Kristen Koske, and they're both qualitative research experts from Cultural Catalyst LLC.

On the cybersecurity team are our SMEs, subject matter experts, all from NIST, Gema Howell, computer security expert; Noah Waller, cryptography expert; and Andrew Regenscheid, also a cryptography expert. So that's our team.

What did we do and why? Well, our original motivator was really the 2022 EAC-NIST-NCCOE E2EV workshop. Now, that is a mouthful. So Election Assistance Commission, National Institute of Standards and Technology, and the National Cyber Security Center of Excellence, where we are today, jointly held a workshop, and it was called "the path to end-to-end verifiable protocols for voting systems." And many of you may have been attendants, but just as a refresher, one of the big things that we heard at that workshop from those panelists was that election officials may not be comfortable with these huge, large-scale, very sweeping technology changes, and instead, may prefer more incremental change.

Another thing we heard a lot about was this idea that election officials are very attentive to and concerned about how they communicate any change, technological or process change, to their voters. So that communication piece, when we're thinking about new technology, is very important, right, hat process, supporting process.

So we had this kind of lightbulb moment. We realized we really want to do some future-looking research with the elections community, understand what are their perspectives, in particular, what do election officials think about E2EV and the future of elections writ large. And what are their perceptions of E2EV

specifically, with accessibility, cybersecurity, and usability, right? And so we knew we wanted to move beyond the workshop and really follow that up with some rigorous qualitative research. And I'll say what I mean about qualitative research in a moment.

And another important thing to consider is we knew we needed to look at that intersection of accessibility, cybersecurity, and usability, so that's why it was so important that we had this multidisciplinary team.

So, to get started, we actually conducted field observations on the use of E2EV in a real local municipal election in College Park, Maryland. And I want to say a huge thank you to everyone who invited us and made us feel so welcome there. That was a huge opportunity for us and very informative. So we actually attended multiple events there. This was back in 2023, by the way. We went to their public information session. We actually observed during voting, during their election day, and then we went to their public tally ceremony that evening, so super informative there.

All right. So let's dive a little bit more into what I mean by qualitative research. There are many different flavors of qual, qualitative research, but here I'm talking about very in depth research interviews that follow a rigorous and repeatable research methodology from start to finish, right? And so we're not just casually like talking to people here. We are gathering rigorously

collected data. So you have a highly trained interview, one who's not just trained, but also well-practiced, right?

They follow a semi-structured interview protocol. And semi-structured means that there's like a core set of questions or concepts that you're covering in each interview for consistency, but then you ask tailored follow-up questions throughout. That interview is recorded and then professionally transcribed, and then it is very rigorously tagged and analyzed by the team. And I'll talk more about that in a bit, but it's a very laborious practice of going line by line through every transcript, and that allows you to find these overarching themes in the data. And that's some of what we'll be talking about today.

And throughout, we applied extensive team experience with qualitative research methods. And I'll say one thing that's really nice about a qualitative approach is it allows you to kind of get this holistic picture, right, so you can think a little bit more than just the technology. What about the people and the processes, that sort of golden triad? And we'll come back to that later.

So why is it important? Well, new voting technologies like E2EV voting systems are being proposed as solutions for increasing voter trust and confidence. So this is all about voter trust and confidence. But it's unclear if these and/or other

nontechnological solutions may meet election officials' needs and address voter trust and confidence.

So that led us to ask two research questions. The first was, what are election experts' views on needs, challenges, and solutions with respect to administering elections and ensuring voter trust and confidence? The second, what are election experts perceptions and understandings of E2EV?

Now, if you're really paying attention, you may have noticed these research questions refer to election experts, but I previously said election officials. Why the switch? Well, knowing that election officials would be just a little busy in 2024 preparing for a presidential election, we opted instead to start our research with experts in the areas of accessibility, cybersecurity, usability, and general elections experts, many of whom were former election officials.

And I'll talk a lot more about the sort of depth of expertise when we get to a later demographic slide, but I do want to point out here that all of the experts in our study, very actively involved in the election space, a lot of years of experience, and, as I mentioned, many were former election officials themselves. So it's a really plugged-in and very well-informed expert group to start our research with.

So a bit more about conducting the study. So, of course, first start with developing research questions. Then you develop your interview protocol based on that, and you apply expert protocol reviewer feedback. And this is a very iterative process, right? You're going around and around and gathering feedback from multiple groups of experts. Now, I want to be clear, these are different experts than those who actually participated in the research, right? And they're all reviewing for a different purpose.

So you have qualitative methodologists, who are really looking at the methodology. How are you asking the questions? Are you phrasing them in the right way, making sure you're not being leading and things like that? And then you have subject matter experts, who are really the experts in the voting and election space. And for us, that meant we were drawing from four expert groups: accessibility, cybersecurity, usability, and general elections experts. I'm going to keep repeating that. By the end of the talk, you're going to have those four groups memorized.

So once you do all that, then you obtain human subjects research approval, right? We get that from the NIST Research Protections Office, where our Institutional Review Board, IRB, is housed. Then you pilot test the actual interview protocol and finally conduct your interviews. Now, this is really important. These interviews were conducted between March and June of 2024.

They're conducted virtually by NIST researchers. On average, they were about 50 minutes, so it ranged from 40 to 60, but the average was right at 50, so just under an hour, which was exactly what we were going for. That's why it's so important to pilot test your protocol, including the timing, and so that's about the interviews.

So once you have the interviews, as I mentioned, they're recorded and then professionally transcribed. And now you have the transcriptions and your actual dataset, so all of that's just to get the data, right? Then you begin, again, this very laborious process of actually analyzing qualitative research data. So that means you're developing, revising, refining a code book. Again, that's a very iterative process where you're operationalizing or defining the codes. Those are the tags that you're going to use to go line by line, every transcript.

And every transcript had two coders, which means that you had two people who were meeting to make sure they're using the codes consistently and making sure we're really coding this very rigorously. And that's important from a qualitative research perspective.

Then you document the findings, right? So all of this, again, I just want to be clear, this was done -- the data collection, the analysis, and the documentation -- prior to the 2024 presidential election. That's important from a timeline perspective. Research

offers a snapshot in time, and so we need to know when that time was. So this is pre-2024 presidential election. And right now, we're in the final publication phase, so please stay tuned for that report. We're putting the finishing touches on it, and it's in the NIST review system.

And I should say that, here, we were going to be focusing on just the each E2EV findings, and there is a much larger report with much broader findings. Shanee will touch on some of those at the end, though.

So I mentioned that we spent a lot of time developing and testing this interview protocol. So what did we actually ask people? So we really focused on eliciting expert perceptions on current and future challenges to voter trust and confidence. Again, voter trust and confidence is really the core here, if any, right? So maybe there were, maybe there weren't. Hint, there were.

And so we asked follow-up questions throughout, as I mentioned, right, some things on like election outcomes, election-supporting technology, what are the three most pressing issues in elections today when it comes to voter trust and confidence and why? What's your personal level of voter trust and confidence? And any potential solutions or improvements to really addressing issues with voter trust and confidence.

Now this is very important methodologically. We saved the E2EV questions for the very end of the interview. That's important because we didn't want to prompt people. We wanted to see whether or not people would spontaneously bring up E2EV as a solution to those challenges that they identified with voter trust and confidence, right?

Another very important methodological point, we did not provide a definition of E2EV, right? We asked people their own familiarity with the concept, briefly describe it in your own words. What are the impacts to voter trust and confidence, if any, and those benefits and challenges, so really trying to look at both sides of the coin here.

And, as I mentioned, we asked tailored follow-up questions throughout the interviews. That means we're tailoring to those four expert groups: accessibility, cybersecurity, usability, and general elections experts.

All right. As promised, participant demographics. So there were four sets of interviews: eight accessibility experts, nine cybersecurity experts, seven usability experts, and nine general election experts. And, as I mentioned, those included former election officials. And I also had mentioned this, but I just want to reiterate, everybody very actively involved in the election space, a very plugged-in group of experts here. So for those of you doing

math, that's a total of 33 election experts participated in 32 interviews across the four expert groups, 32 interviews because one interview had two experts in it.

So self-reported years of election experience ranged from a minimum of 10, so a minimum of a decade of experience to over 40 years. The average was around 23 years with a standard deviation of about eight. And so looking across those four expert groups, they had a total of over 650 years of combined election experience. So I don't think anybody can argue that this is not a highly expert group.

Range of backgrounds: academia, industry, government, nonprofit, election organizations, and standards works.

So I mentioned that we get human subjects research approval from the NIST Research Protections Office, so I do want to talk briefly about data protections. Participant data has been deidentified by assigning a participant code. So you'll see things like A-1, C-1, U-1, G-1 where the letter refers to the expert group so you know when we present a quote what expert group it's coming from.

And, as stated in our human subjects research approval, the research team will not make any attempts to reidentify study participants or link anonymized data back to specific individuals. This is standard research practice for us. We do this for any study.

But we also know that the voting community is very small, so it's particularly important to protect participant anonymity. Therefore, please do not like self-identify if you participated or you think you know somebody who did.

All right. As promised, I did want to step through a formal definition of E2EV from the literature before we present results. And this is from a Benaloh et al. 2014 paper. So E2EV systems are typically defined by three technical properties, and we'll step through each of these: cast as intended, recorded as cast, and tallied as recorded. And sometimes the language varies a little bit, but these are the sort of three principal concepts.

So cast as intended: Voters make their selections and at the time of vote casting can get convincing evidence that their encrypted votes accurately reflect their choices. So cast as intended.

Recorded as cast: Voters or their designees can check that their encrypted votes have been correctly included by finding exactly the encrypted value they cast on a public list of encrypted cast votes, recorded as cast.

Now, tallied as recorded: Any member of the public can check that all the published encrypted votes are correctly included in the tally without knowing how any individual voted, right?

So we'll refer to these as like the three key properties or characteristics of E2EV voting systems. And, again, I just want to highlight that methodological point. We did not provide this definition to participants, right? That's very important. So that's the formal definition from the literature. Let's hear what the experts in our study had to say.

So I want to be very clear that the data I'm about to present are views/perspectives from the election experts we interviewed in our study. I'm not presenting NIST's views on elections or E2EV. These are our data, and you'll see they're either presented in summary format or using quotes verbatim, and those are representative quotes from the larger dataset, so that's called exemplar quotes.

All right. First and foremost, E2EV was not top of mind for most participants. So many of the participants discuss E2EV only when specifically prompted at the end of interviews. However, E2EV was mentioned organically or spontaneously in a few, right? And those people would often comment on both the positive and the negative potential for E2EV to impact voter trust and confidence. And so, as mentioned organically in 11 of 32 interviews, and six of those 11 were from cybersecurity experts, and so it did seem to be a bit more top of mind for the cybersecurity group.

We heard a lot of uncertainty. Many experts expressed uncertainty when describing E2EV. Accessibility experts, usability experts, and general election experts expressed that they weren't 100 percent sure exactly how the technology works, and so they'd say things like, "Well, that's my understanding," or "I'm not really sure." So we heard a lot of qualifiers when people were describing it, and that's true for just over half of that expert group. So accessibility, usability, and general elections, just over half of them expressed some type of uncertainty.

Interestingly, however, despite their uncertainty and kind of reservations, they could largely articulate at least one of those three key properties that we talked about on the formal definition slide. So even though they're a little uncertain, they still kind of know about the concept. And so we'd hear things like, "I'm never quite sure of E2EV verification, but in general, that's my understanding," so we'd hear a lot of those qualifiers. That was from an accessibility expert A-1. And often, they were referring to the sort of complexity or perceived complexity as a reason why they weren't really sure exactly how it worked. So we'd hear things like, "There's a ton of complexity underneath the hood." And that's from a general elections expert G-9.

Interestingly, no uncertainty expressed by cybersecurity experts, right?

[Laughter]

MS. GREENE:

I hear people laughing, right, but they were very matter of fact in their definition. So none of the nine cybersecurity experts expressed uncertainty.

I also want to point out on this slide, when we are displaying in these quote bubbles actual verbatim quotes from our experts, followed by the participant code in parentheses, so, again, that'll tell you what expert group they're from. And these are exemplar quotes, which means they're representative of the larger dataset.

We heard a lot of differing perspectives, right, probably not surprisingly. Experts held differing perspectives on both the benefits and the limitations of E2EV in relation to voter trust and confidence in elections. Interestingly, that divide was not always consistent across expert groups. So you might be thinking, well, since E2EV is all about cryptography, it has this cool crypto in it that all of the cybersecurity folks are going to be very positive about it. That was not actually the case where we had some cybersecurity folks expressing doubts about the efficacy and practicality of E2EV and the reverse, noncyber folks, you know, expressing support.

So I'm going to show a couple differing perspectives here, and these are both from cybersecurity experts on the left from C-3. "Instead of telling voters that they should trust the results, there are

good people doing it, don't worry, we should be giving voters direct evidence so that they can see for themselves that their votes are being accurately counted," versus, again, from a cybersecurity expert, different one, different perspective, "I no longer think that we'll have a truly, fully end-to-end verifiable voting system where voters can independently verify the entire path. I don't think that it's doable at scale. And by at scale, I mean scaling to the breadth of knowledge of individual voters, too confusing for most voters."

All right. This is the only table in the presentation and in the larger report. In general, we don't really like to quantify qualitative data, right? They are fundamentally different data types. They serve fundamentally different purposes. Nonetheless, it is sometimes valuable to present, you know, some summary numbers, and so that's what we're doing in this table. We're presenting experts' overall sentiments toward the potential of E2EV to influence voter trust and confidence, right? So we've been people by those four expert groups, and then the sentiment I refer to as either largely positive, largely negative, or noncommittal, right?

And there's an N of 27, total N here of 27 rather than 32 because this wasn't addressed in every single interview.

So I just want to kind of hit the highlights here. So you'll see a total seven of 27, largely positive. I don't have my slide notes. I

think that's like 26 percent. Twelve of 27, largely negative. That's about 44 percent. Eight of 27, noncommittal, right, so pros and cons. And that's about 30 percent. So that's the totals. And you can see that largely it's kind of split within, you know, the expert groups.

But I do want to point out the usability experts in the penultimate column here. Only one largely positive, six largely negative, and zero noncommittal. Now, kind of compare and contrast that with the cybersecurity experts, where you have three largely positive, two largely negative, and four noncommittal. So there might be some potentially interesting differences, you know, between groups and between experts. I think the more compelling story is really in those totals, seven of 27 largely positive, 12 of 27 largely negative, eight of 27 noncommittal. And the really interesting thing is, why noncommittal, right? You know, these pros and cons, and people are, I think, very aware of both sides of the coin here.

All right. So I hit some of the highlights. I'm about to hand it over to Shanee for a deeper dive, and she's going to talk about four different areas, support for evidence-based elections, concerns about complexities of E2EV, which I alluded to, the need to support modern and accessible voting technologies, and the overall value proposition of implementing E2EV technology.

MS. DAWKINS:

All right. Thanks, Kristen. As she said, I am Shanee. Good to see you all. And I'm going to walk through some of the key findings we have in these four groups on the slide. Sorry that some of the slide is a bit covered up by a link that's not going away there, but I will read what's on the slide so we should be okay here. And let me get set up here. Okay.

So I'm going to start with support for evidence-based elections. So some experts, particularly in cybersecurity, advocated for more evidence-based elections in our data. So they believe that E2EV has the potential to engender voter trust and confidence by providing evidence that election outcomes are accurate. However, other experts believe that getting voters to take the extra verification steps may be difficult.

And so I have a quote here from usability expert who said, "The mental model that most people have of how to vote is you make your selections and submit them, right? And that's the end of the game. So E2E systems, in order for them to actually do what they want to be doing, require at least some number of voters to perform extra actions, right, to do verifications and to do whatever. And I think it's always a challenge to motivate voters to perform those extra steps." And that's from participant U-5. So the extra

verification steps are optional, but assurances for E2EV systems are dependent on enough voters actually performing those steps.

And so some experts also noted that E2EV systems have limitations if an issue is detected. And again, particularly in cybersecurity, we're able to express this during the interviews. And so I have some quotes here from cybersecurity experts, one who said, "The verifiable technologies that we have are all about detection of anomalies. They're not about prevention. They're not even about recovery." And that's from participant C-3.

And then the next quote here, a cybersecurity expert said, "If you discover that something went wrong, what you get is that, oh, the system doesn't actually verify the correct count, and so it's got a large potential for a relatively small error to appear that the election has been completely compromised, and that actually has the potential to make things worse rather than better. That could unnecessarily decrease confidence in what may be a moderately flawed but fundamentally sound election procedure." And that's from participant C-4.

So experts in general noted that E2EV technologies are essentially a type of after-the-fact auditing mechanism and are not proactive, and that could negatively impact voter trust and confidence in elections and election processes.

And so, next, we'll move on to complexities of E2EV. So experts across the four groups that Kristen mentioned many times that E2EV introduces another layer of complexity to elections and may be difficult for voters and election officials to understand.

One of the cybersecurity experts said, "E2EV systems leave the voter with a receipt, and they are generally very clever to prevent that receipt from actually revealing to a third party how someone voted, but they could create the impression among voters that their vote isn't secret anymore." And that's from participant C-4.

And then a general election expert said, "People don't understand hash values, and so all of a sudden I'm getting this string of codes. It's like, this isn't what I wanted. What I wanted was to see my ballot in the ballot box. Well, no, we can't do that because of X, Y, Z and ballot secrecy and so on and so forth." And that's from participant G-4. So even participants who are largely positive about E2EV acknowledge that people wouldn't understand the math behind that technology.

And so, again, across the board, experts emphasize the need for effective communication and education about E2EV. So some experts believe that communication and education about E2EV could counter the complexity issues and positively impact voter trust and confidence in elections. And so a cybersecurity

expert said that "Communicating kind of how the process works from end to end and breaking down the technology behind it, I think, is where the real challenge lies, right there." And that's from participant C-9.

And a general election expert said, "Explaining the math behind cryptography in E2EV is not worth the time for most people, but explaining, here's how we know your vote was counted as cast, that's worth the explanation. I don't need to give you the equations, but I do need to walk you through more than just 'trust us, it's in there.'" And that's from expert G-5. And that also reinforces what we learned when we observed the College Park elections and the importance of communicating and doing voter education during the elections about E2EV systems.

All right. So, next, I'll talk about modern and accessible voting technologies where some experts believe that E2EV could enable the introduction of more modern and accessible voting technologies. So a cybersecurity expert says, "I feel like we can make voting more exciting and accessible really easily with end-to-end verifiability." All right. So this is cyber expert C-1.

And then we have an accessibility expert who says, "Maybe we can embrace some better technologies if we really got serious about end-to-end verification. I think if we use it as an opportunity to make people feel more secure about newer technologies, then it

could have huge benefits for everyone." And that's participant A-3. So some experts felt like innovations enabled by E2EV could support easier and more accessible voting mechanisms for elections.

However, many experts believe that, despite this promised support for more modernity, voting technologies implemented using current E2EV systems are often not fully accessible, and this is in large part due to the handling of paper during the voting process. So a usability expert said, "I've not seen a demonstration of an end-to-end verifiable system that is accessible. They haven't figured that out to my knowledge." And that's participant U-4.

And then a cybersecurity expert said, "I feel like nobody who cares about accessibility and true independence has to explore non-paper-based methods to really enable that for meaningful segments of the population. I think that's the thing I feel is truly missing in this discussion. It tends to focus on security, not access." That's really what it says under there, so apologies. And so that is from a cybersecurity expert about the accessibility of E2EV systems.

All right. And then, finally, we have the last area. Here is overall value proposition of E2EV. I know we're presenting a lot of data here, a lot of quotes, but we'll get through this here. So experts believe that it may be difficult to show the purpose and

benefits of E2EV and challenging to convince voters, election officials, and vendors of the value of adopting E2EV systems.

And so I'm going to step through the sub-bullets here as some of the views expressed by our experts during the interviews, starting with what problem E2EV is solving. We have a quote here from a cybersecurity expert who says, "E2EV is a solution in search of a problem," a very succinct quote. That is a sentiment expressed throughout our interviews.

And then we have the voter point of view, where several participants did not think E2EV addressed voter issues and the issues that voters are most concerned about, right? So we have an accessibility expert here that says, "I think putting end-to-end verification on top of already-existing systems makes computer scientists feel better" -- I'm a computer scientist -- "and that's it. I don't think it even makes regular voters feel better because they don't know what it is and they've never thought about it, and I think they don't care." And that's from accessibility expert A-3.

And then we have a usability expert who says, "If you look at surveys, most people believe that their votes were counted accurately. That is not the issue about where their doubts are coming from. It's whether other people were able to vote and their votes shouldn't have been counted or there were a lot of extra votes that were counted in the election, that kind of thing, where

there seems to be confidence issues." It says something like that under there. That's from U-2.

And then, finally, we have some participants who believe that it might be challenging to make this value proposition to election officials who must ultimately decide to use E2EV in their jurisdictions. And we have a general election expert here that said, "If election officials can't understand it and explain it, they're not going to use it because they know if they introduce something new that they can't explain, they're inviting criticism and conspiracy, right? Election officials ask me all the time, 'Am I introducing more problems, or are you solving a problem for me?' And I think that it's solving a problem for them from a trust, transparency, and validation point of view. But if they don't believe that they can explain that, it's going to do them no good." And that's from participant G-5.

And so while participants noted that finding election officials willing to pilot E2EV systems in their elections has been difficult, several mentioned that some have been used in a few smaller elections in the U.S. And those are on the slide here, starting with Tacoma Park, Maryland's municipal election in 2009; Fulton, Wisconsin's municipal election in 2020, a little more recently; Franklin County, Idaho's general election in 2022; and then finally,

the election that our team observed in College Park, Maryland, for their municipal election in 2023.

And so despite their skepticism about the potential of E2EV, several experts noted the demonstrated success of using the systems in real-world elections, and they also emphasized the importance of good communication and voter outreach, as we previously noted that we observed in the College Park election.

Now, a few participants noted that these implementations have provided positive proof that E2EV does not detract from voter trust and confidence in elections, but they have not necessarily shown that E2EV improves voter trust and confidence in elections, right? And so some experts believe that if E2EV is more widely implemented, people may come to trust and value it.

And so I have a quote here from a cybersecurity expert who says, "How many times have you gotten on an airplane? And did you understand what it takes to make an airplane safe? And of course, very few of us do. Well, so why did you get on the airplane? You had experts that you believed in or friends that believed in experts or experience over time." And that quote is from participant C-8. It's a very common analogy used in voting for the airplane, but it breaks down a little bit on some level, right? So people may not understand how airplanes work, but they generally know what they do. They get you from point A to point B through

the sky, right? But that can't always be the same for E2EV systems, which people don't necessarily understand the math behind the technology and how that works.

But as the participant C-8 alluded to here, "It's a demonstration that the technology works in practice, and authoritative and trusted messengers and experts who vouch for E2EV may improve trust in the technology."

And so many experts believe that E2EV is not the panacea for increasing voter trust and confidence. "E2EV is not going to be a silver bullet," and that's a quote from participant C-7, a very succinct quote from a cybersecurity expert.

We have a general election expert who says, "I'm not opposed to it. I'm not against it. I think adding layers of defense, providing people opportunities to be able to build that trust is a good thing, but it's definitely not the panacea." And that's from participant G-4.

And then a usability expert said, "It's hard for me to believe that there's a magic technology that's going to suddenly make everybody go, 'Oh, I've seen the error of my ways, our elections are great.'" And that's usability participant U-1.

Okay. And so that walked through the four areas, so a summary of those findings, right? When considering the implications for voter trust and confidence, first, we have to look at

expert perceptions of E2EV's influence, right, where the benefits the experts said that it has the potential to increase voter trust and confidence. Great. Their concerns are that it has the potential to decrease voter trust and confidence by introducing additional complexities that could then be misunderstood or even intentionally exploited in the information environment.

And we also have to consider the perceptions of the E2EV technology itself, where experts said the benefits were that E2EV offers important properties for election integrity. They also said their concerns are that it requires a shift in voters' mental models, including that extra verification step for one of the important properties of E2EV to be fully realized.

All right. So in wrapping up these findings, E2EV technology is intended to improve voter trust and confidence, right? This is something we said. It's not something that just the experts said. The EAC-NIST-NCCOE E2EV workshop that Kristen mentioned a few years ago was the original motivator for this research study, right? During that workshop, panelists indicated that widespread adoption of E2EV may not solely be dependent on technical protocols, requirements, and evaluation criteria of E2EV. Election officials expressed concern over large-scale, sweeping changes and preferred incremental change, something Kristen also mentioned earlier on the slide. And then, finally, panelists during

that workshop also noted that E2EV technologies have not been fully accessible for voters with disabilities.

And so our data suggests that there are more pressing issues facing election officials today than those specific technological challenges that E2EV could potentially address. And I have a quote here from a cybersecurity expert. "The biggest challenge is that E2EV is this beautiful technical solution to something that I'm not sure is recognized by society as the biggest shortcoming or the biggest challenge with elections right now." And that's from participant C-2.

So E2EV was not top of mind for most experts in our research, as Kristen mentioned. Few experts even mentioned E2EV unprompted as a potential improvement for voter trust and confidence or as a future technology in elections.

But that leads me to what the experts thought were the priorities for improved voter trust and confidence in elections. So there's a lot on this slide. This is an infographic pulled from our larger report on our broader results from the study that I'll walk through. It's important to situate our E2EV findings within the larger voting landscape, and to point out that our focus on E2EV today is not commensurate with the salience in our data, right? The experts spoke about many other areas for improving voter trust and confidence in elections.

So, overall, I want to start with challenges. Voters expressed more pressing challenges for voter trust and confidence in these areas here: limited or incorrect voter knowledge and understanding about elections; the need for technology that is usable, accessible, and secure; unrealistic or unmet voter expectations about elections; and sufficient resources for election officials, in those four areas.

But they also noted improvements that align with one or more of those challenges, like technologies to increase voter trust and confidence in elections, enhance voter communication and education related to elections, greater recognition and support for the election official profession, and then increased resources for election officials.

Now, voter trust and confidence -- I'm going to jump down to this gray area at the bottom -- is influenced by external factors such as the complexity of elections in the information environment. External factors permeate the world of voters but are largely outside of the control of election officials. Voter trust and confidence is also influenced by a variety of challenges that I mentioned earlier, some of which can be addressed by election officials through the advancements and improvements that I mentioned that are on this slide as well.

And so all of this ultimately impacts election officials and what they do, right -- we're going to the middle section here on election officials -- who face multiple challenges as they work to facilitate elections. They are the connective tissue between elections and voter trust and confidence. But election officials need help to implement current and future improvements in elections. And, of course, all of this is colored by the information environment surrounding elections and the complexities of election technology and election processes.

So this infographic is pulled from our larger report on our study results, and that will be posted to vote.NIST.gov. It's in the system, we're finalizing it, and it'll be posted very soon. Please stay tuned there.

All right. And so to ensure successful deployment, widespread adoption, and trust of new technologies, you must consider the golden triad, right? That's people, processes, and technology. Election technology, including E2EV, should not be developed in a vacuum. And in a sentiment expressed in our interviews, care and caution are needed, especially when substantial changes add complexity and are difficult for voters to understand.

And so a cybersecurity expert said that, "We probably have to weigh technological improvements against whether that's going

to degrade confidence." And that's from expert C-4. Another cybersecurity expert stated, "Getting the technology right is important, but second in importance to the institutions of trust and the perception and designing systems that people can understand and feel confident in." And that's from cybersecurity expert C-2.

And so this is the reason we took the time to conduct this research, right, to systematically collect the data, understanding a variety of viewpoints and considerations for voter trust and confidence in elections. And so we hope our data today will facilitate thoughtful discussion here and in the future on voter trust and confidence in elections in E2EV.

And I just want to leave you with one quote to sum up our findings about the expert perceptions of E2EV use in elections. "You can't create voter confidence with math." And this is from a cybersecurity expert C-7.

So voter trust and confidence is multifaceted, right? It's not one single thing, but many things over time that build that trust and confidence. And you can't just focus on the technology. Any new voting technology and election processes, you have to think about the communication, education, voter outreach, and really consider the golden triad of people, process, and technology when developing systems.

All right. So thank you. Again, stay tuned for our full report on all of our findings. It was a lot of data to go through, but we're really excited about the full report, and I think, hopefully, we have time for some questions.

MR. SKOGLUND:

Kevin Skoglund, representing IEEE. Your predecessor mentioned the makeup of the experts. I didn't hear explicitly whether any of those people had actually been involved in E2EV projects in some way or not because, obviously, there are a lot of cybersecurity experts who are also working on those areas.

MS. DAWKINS:

Right. So we didn't explicitly ask if they were involved in E2EV. That wasn't one of our interview questions. But, yes, some of our experts were involved in E2EV in some way. And, again, we're focused on what their thoughts about the benefits and challenges of E2EV. Do you have anything to add, Kristen, for that?

MS. GREENE:

No.

MS. DAWKINS:

No? Okay.

Yes?

COMMISSIONER PALMER:

Thank you for the presentations on this. I think it's sort of a circular argument because you're looking for evidence, you're looking for evidence-based elections, plus the transparency that this technology could provide. But one of the issues you hear all the time when you're talking to very intelligent people, voters sometimes, it's if I don't understand what's happening with the voting process, how can I trust it?

And I do understand the fact that if you don't understand how it's providing the transparency or the evidence that it's a circular argument, and so I'd love to hear from the voters, their responses after using the process because, you know, for a long time there was this long discussion about, I need receipts, I want to have receipts, I want to be able to visualize that my ballot was counted. But, you know, that's sort of -- you know, you don't hear that as often from the public, but there is sort of this need to, how do we provide transparency of the security and the confirmation of their vote generally? And so, you know, I would love to hear what the voters thought after going through the process.

COMMISSIONER HICKS:

I will also say that's a sneak preview for some of the afternoon conversation, so look forward to that.

MS. DAWKINS:

Yes, I think in some of the real-world implementations of E2EV in those smaller elections, they have done some discussions with voters, exit polls, and so they have written reports on what voters think, and I think you'll hear from those folks later today. We did not interview voters directly, so we don't have direct data to give insight into their thoughts about E2EV specifically. But I think, like Ben said, we'll hear about that later today.

COMMISSIONER PALMER:

Thank you. And it is really a challenge for election officials and even the EAC to sort of articulate how our voting systems are developed, how they're tested, and how they're deployed, you know, so that's always going to be a communication challenge.

MR. WAGNER:

Dave Wagner here. I wanted to thank you. I wanted to thank you both for your work on this. I am really impressed by the quality of the work you did here, the research, and also the clarity of your presentation and taking on such a complex subject. I think this is really great stuff. I really appreciate that you're distilling the wisdom and the expertise and the perspectives from all these different communities that you've been interviewing and able to identify a whole bunch of insights for us from this, so I feel like we're really fortunate, and the nation's really fortunate to have your work, so thank you.

MS. DAWKINS:

Thank you very much, appreciate it.

MS. GOLDEN:

I'm going to pile on with the same thank you from a completely different perspective. I just appreciate including accessibility, completely separate from usability, which is a soapbox I've been on for 100 years trying to distinguish that for people so they understand they are not the same thing at all or in many ways, but also because it's so glaringly clear. I'll go back historically. So I think E2EV -- I'll get the new terminology right -- came in with software independence, which, in my humble opinion, was a euphemism for a paper mandate. And I think we're couching things because we didn't want to say outright, you have to have a voter-verified paper ballot. But we're there anyway, and so this whole software -- and so it was there because of the accessibility problems of a paper ballot, which continue to daunt us.

And yet, it's proving to not even be accessible as an E2EV, just the whole thing, talk about a circular argument. We got here at least partly trying to circumvent the paper ballot inaccessibility problem with something that would let us go back to a digital ballot, which has caused its own accessibility problems. It's just this, you know, circular problem of, yeah, security and accessibility naturally butt heads, let's face it, and so every time you think you've got a

solution, it's probably not going to be that simple to solve the balancing act between security and accessibility. And, you know, you approached it in a structural, solid way for dealing with qualitative data. And I truly, truly appreciate it, and I look forward to reading everything.

And just FYI, I think I can probably identify all your accessibility people just by the terminology. I know exactly who that was, and I will be talking to her later. And I know the two people. I can identify them. I'm 99 percent sure, so thanks.

MS. DAWKINS:

We cannot confirm that you will be able to do that.

[Laughter]

MR. SCHOELLER:

Shane Schoeller, Board of Advisors. A couple things. First of all, I like the plane analogy because there's some people who will not fly in a plane. If voters don't trust it, will they participate? I think that's something we have to consider. Planes do crash, just FYI. I hope never to be in that situation, but they do.

And then, secondly, does end-to-end voter verification system actually protect the voter from coercion and intimidation? Is that something that we've considered? Because that's something we've had a huge issue in Missouri in years past, and so we put

that into consideration in terms of making sure the voter is protected in terms of being able to vote in that type of a system.

MS. DAWKINS:

Are you asking us if those systems protect against coercion?

MR. SCHOELLER:

You're welcome to answer it if you'd like.

[Laughter]

MS. DAWKINS:

Just clarifying.

CHAIRMAN HOVLAND:

I'll chime in with a couple things. I guess, first, before I make a long statement and people forget what I'm talking about, I did wonder if you could expand on or if you had insight into the usability expert sort of negativity. Or when you put up the slide that, I guess, six of the usability experts reacted negatively, was that based in like the complexity of the math and sort of people's general understanding of that or process? I was just curious if you got more insight into where that was coming from.

MS. GREENE:

Actually, that's a great question, and thank you so much for that. And thank you for all the questions. There were a lot of different reasons, right? And so we go into a lot more detail in the larger report, but a lot of it did have to do with this concern around

changing voters' fundamental mental model, right, that you're asking them to take another step, a verification step. It is optional, but if you want the assurances of E2EV, you need some people to do that, right? So there is concern over sort of that additional step.

I think a lot of people also, you know, are more familiar perhaps with older implementations of E2EV, and we know there's been improvements in terms of usability, but that concern over the additional step and that hurdle of getting people to change, you know, a decades-old mental model, right? You look at how long, you know, many people have been voting. They've been doing it a certain way, and now you're asking for an extra step. And getting people to participate in general is hard, and now we're asking for a little bit more, please.

And so I think that, combined with the complexity and concern of that communication and outreach, and that even if we are able to successfully tell people how to vote with these systems, which has obviously been done in these real-world elections, do they really understand the enhanced security properties? Do they understand why they're taking this additional step? Maybe it doesn't matter. But, you know, these were just some of the concerns that experts had expressed.

They also even alluded to the fact that, well, they're not fully accessible, so, you know, you're not necessarily gaining something

there, at least in current implementations. And so, yeah, very multifaceted. Thank you for that question.

CHAIRMAN HOVLAND:

Thank you. And sort of some of what it made me think about in Diane's comments and for, you know, a sneak preview for the afternoon conversation, I think this presentation is extremely useful in framing the complexity of this technology and of implementing this. But I think, you know, also, I mean, the trust piece is a big deal. It's something that I know we always think about, election officials always think about, but our social scientist friends also told us long ago and have been reaffirmed that the outcome of the election and people's relation to that dictates so much of a more significant percentage of trust than probably most other factors, so we are aware of that.

But also, as Diane highlighted, you know, thinking back to the 2.0 conversations and adoption, I mean, this is in 2.0 because of software independence, because of having a pathway, and we see election officials in the elections community also looking at this for solutions to serve voters outside of the scope of the VVSG in other systems as well.

And so I do think that, as we think about both the presentations this afternoon and then our conversation, you know, I do think it's important to remember the complexity and then think

about, you know, yes, security and trust is a piece, but accessibility is the primary reason that this is in the VVSG as far as I understand.

And then, you know, how do we navigate these challenges, particularly for this body, as someone who certifies voting systems? And so ultimately, what do we need to be looking at or testing to to understand that these systems can work and can serve voters?

So, again, appreciate the tee up for the afternoon's conversation, but, again, this is obviously -- again, it's a nice frame that this is a tremendously complex issue and subject matter, and I say that as someone that isn't that good at math.

Any other questions?

MS. GREENE:

Could I just follow up on something that you had mentioned? Our experts -- this is something that permeated the data across all expert groups -- mentioned exactly that issue that you were talking about, that voters tend to trust more when their preferred candidate wins, trust less when their preferred candidate loses. And so there's a certain component of variation in trust among the voters that we're not going to be able to do anything about technologically, right? And so I think that that idea that technology isn't the silver bullet, it's not the panacea, but it's something we still have to get right was really, really important. Thank you.

CHAIRMAN HOVLAND:

Thank you. I think we have a little time to jump forward and get the first presentation that we were going to do after lunch before lunch so maybe you all can beat some traffic for those of you who are driving. We might go ahead and do that, so we're going to have Ben Jackson, who's a senior subject matter expert at the EAC, come up and do a presentation, and, again, timely to the conversation we were having, thinking, again, back to the 2.0 conversations. What Ben is about to present on is something that grew out of those conversations, frankly. Diane highlighted some of the shortcomings of HAVA and particularly the one-per-polling-place standard of that.

At the EAC, we know that there are certain things that are beyond our control, and we are not in a position to rewrite HAVA, but we are in a position to look for ways to support the elections community, and one of those areas related to this Ben is going to talk about now, so, Ben, take it away.

MR. JACKSON:

Thanks, other Ben.

[Laughter]

MR. JACKSON:

That was somewhat self-serving, but note, you teed it up perfectly. My name is Ben Jackson. I am one of the senior subject

matter experts at the EAC, but my focus is on accessibility. And so prior to joining the EAC, I was a staff attorney at Disability Rights Maryland, where my work was funded by HAVA to ensure election accessibility from voter registration through mark casting and verifying ballots.

And, yes, to Ben's point, there's been, you know, consistent conversation for the past 20 years on how to deploy assistive technology to voters with disabilities and understanding that HAVA does set the minimum threshold of one accessible machine per polling place, but is that enough to serve voters in an efficient way? And so this was something that I worked on with the state and local boards of elections in Maryland, and so, initially, it was just trying to determine how many voters with disabilities exist in precincts.

And so, fortunately, we were able to come up with a tool that addresses that, and then, using that information, we've come up with another tool that's still in beta testing to implement that to determine how to optimize the deployment of resources.

So the first tool is on our Learning Lab platform. The Learning Lab is available to election officials across the country. It's currently online, and it has a short video training series. They're designed to be practical and include best practices, and they have a variety of topics, including accessibility.

And, to Diane's point, I'm currently working on a script for ADA title II and how the Department of Justice memo that was released in April of last year will apply to local election officials, and so trying to distill down what those standards are for web and mobile content accessibility and what that means to election officials. So you're a little ahead. That'll be out, again, hopefully later next year, but this is a resource that is currently available on the Learning Lab platform is how to determine the voting age population of voters with disabilities.

And so this is it. We're just showing election officials and policymakers that they can go to data.census.gov. They can enter in disability. For this example, we're using Michigan, and then we're using cities because that's how the jurisdictions work. That's how they do their population in Michigan. So, yeah, so you type in the locality into the search box here. And the user interface has changed a little bit on the website, and so we're going to work on updating that to go through.

But drop down, you select the city, you have the disabled population for the city, which is 15.4, but that includes the population under the age of 18, and so this is just going in and showing here's how you view the results. And then for the rest of the video, you'll see that it also includes gender, race, ethnicity,

other demographic breakdowns that are not necessarily pertinent to election officials.

And so, you know, I'm talking a little bit faster than I click through this. So, yeah, you want to get rid of this information and stick to, you know, the breakdown, and it includes the margin of error, so we're going to remove the margin of error there, also removing the information for gender, and then -- yep, so now we have this information, and then the rest of the video just goes on to show that you're going to add the total population for 18 to 75 and older and divide that by the estimate of people with disabilities.

And the video does go on to say that this doesn't include potential voters who are institutionalized, so it's just giving you a rough estimate of the percentage of voters in your municipality. So based on this data, this is data that's, you know, readily available, publicly available.

I had these conversations with the state and local boards of elections in Maryland, and so we're just trying to estimate, okay, you know, using more simplified math, we can estimate that, okay, 16 percent of their voters are going to be people with disabilities, so if we have, you know, 10 voting booths, you know, based on the population, we could probably have two of them being accessible to voters with disabilities so that we don't slow down lines. But I think it was a static calculation, and it wasn't necessarily based on what

election officials can add to knowing, you know, their voting population more specifically.

So, fortunately, we were able to partner with the University of Rhode Island to create this accessible voting systems calculator, and so the University of Rhode Island has timed elections across the country for the past three or four federal election cycles, and they were able to calculate how long it takes voters across the country to vote, and then, using that information, they simulated millions of voter experiences across the country, and so you can take that percentage of people with disabilities, and you can enter it into the demographics calculator in this model, and you can run the simulation, which I will play for you now.

So, yeah, so once you get to the Census Bureau, then, you know, the local election officials can enter in the number of voters that they think per precinct the percentage population of people with disabilities and then the target maximum wait time. Again, this tool is still in beta testing, but, yeah, this is going to be similar to, hopefully, what we have finally.

And then for the check-in stations, whether you do it electronically or by paper, the number of voting systems both accessible, starting with the minimum threshold of one, and then the number of maybe hand-marked stations, and then you're going to run the simulation. And it also has the type of ballot casting

equipment there, either using the electronic ballot scanner or a ballot box. And then you will get the results.

So the results show the average wait time based on what technology was currently deployed would have given you 53 minutes average wait time with a check-in of 36 minutes. And then there's the graph there showing the same results. But the graph and table are both there, again, for accessibility purposes. It's easier to read this in table form than it is graphically. And then the accessible machine wait time is a few hours, so probably going to be an inaccessible voting experience. But it takes, you know, two minutes to vote.

And so then the optimized result says that, you know, based on this, you should have additional check-in stations, which will reduce the further wait time. So once you enter in additional check-in stations, then you can take a look and see that the average wait time has decreased to 21 minutes with a wait time of two minutes, and it gives you the original results and the optimized results.

And so, realistically, you know, this was borne through research that I had done prior to joining the EAC. I was trying to find, you know, knowing that there's a minimum of one per polling place, how many voting systems should be deployed to optimize times? And I found deep, deep, deep in a congressional record

that somebody had proposed a 1 in 10 ratio of hand-marked or inaccessible ballot-casting stations to accessible stations. And so I emailed this person and then set up a phone call and was like, how did you come up with a number 1 in 10, and they said, well, it's more of an art than a science. And I didn't particularly think that that argument carried a lot of water.

And so, fortunately, by joining the EAC and partnering with you, we have turned what was an art into a science. And so, hopefully, this will give policymakers, election officials, a more evidence-based and data-based approach to deploying what existing resources they have, procuring additional resources in the future so they can optimize the wait times and the voter experience for voters with and without disabilities.

And then to cover the NIST implementation, they did a great job of highlighting this earlier this morning, but these are some of their papers, and I think they do dovetail fairly well with the resources that we're putting together, including their presentation on assisting voters with disabilities in polling places, and specifically their slides on how to implement different accessible voting machines and polling places.

That's been feedback that we've received from poll workers and election officials and voters with disabilities is that the technology might not be turned on or readily available, and some of

that is due to unfamiliarity with the technology. And I think this presentation does a good job of being able to be customizable to the local jurisdictions so that you can put in examples and pictures of the specific type of technology that's using that polling place to help poll workers gain confidence in that technology, understand the assistive features that exist and how to use them to hopefully reducing those kind of last-mile barrier details.

You know, we're doing a pretty good job, based on our research and data. Over the past 20 years since HAVA has been implemented, we have reduced significantly the barriers to voting for individuals with disabilities. But, you know, while the machines be deployed, people might not be familiar with the technology, and then that's going to make the voting process inaccessible. And so I think this carries it kind of over the finish line there of, you know, ensuring that people are comfortable with technology, know how it's used, and can operate it.

But, yeah, now I will answer any questions you have, unless you are overly eager for lunch.

CHAIRMAN HOVLAND:

And while people think about questions, one, Ben, thank you for the presentation. And two, I'd just like to highlight, I think one of the things that is exciting about this -- or, you know, obviously HAVA has the one-per-polling-place minimum standard, but also

HAVA now has -- it's been a little while since that was passed, and we've seen a lot of evolution in how elections are administered, you know, and certainly not all polling places are built the same. And whether that is, you know, a rural township somewhere that administers at the municipal level to, you know, again, particularly post-HAVA, we've seen the emergence of vote centers. And so if you've got a vote center that you're expecting to serve 10,000 people, that's a very different circumstance.

And so I think one of the things that's very nice about this tool is that it allows people to play with those numbers. It allows election officials to think about that, again, particularly if voting in their jurisdiction is changing, if vote centers are new to their jurisdiction, you know, or, for whatever reason, maybe with a redistricting, their particular site is changing the number of voters it's serving. And so, again, you know, trying to provide resources that help officials to serve their voters and think about issues like this, so thank you again, Ben.

And anyone that has questions or feedback would welcome that.

MR. SCHOELLER:

Shane Schoeller, Board of Advisors. In terms of the model you have there, there's no additional wait time for someone that needs accessible voting equipment, at least where I'm at. What we

find is curbside voting has been a challenge, and that's because they have to take the check-in equipment, the ballot, and everything to the curb. And so I know even based upon 2024, the polling locations -- because we added additional polling locations to reduce wait time -- but we had probably four or five at most where we had more curbside voters who were going to have just a check-in team just for the curbside voters.

But I don't understand the wait. Regardless of the vote, you're going to be checked in. Matter of fact, what I did in our county was we now use the accessible voting equipment for every election. It's not required in local elections, but I did that in order to increase familiarity for the ExpressVote operators. We use the ExpressVote system in Greene County.

Then, additionally, I incorporated testing so you have to pass a test before you're able to operate the equipment because we have the issue in terms of sometimes they were not familiar or they wouldn't turn it on, and they don't get paid if they don't turn it on. But I've worked with the visually impaired and blind community frequently, matter of fact, go to the regular meetings. They have really appreciated what we've done. So I realize I may be an exception to some.

But I'm really having a hard time grasping why check-in time would be different because they're in line just like everyone else. I

see it for curbside voting, but I don't see it for why it would take longer to check in a voter who needs accessible voting equipment than it would anyone else.

MR. JACKSON:

Sure. And so, again, it depends on your voting situation, and so the backup there for the check-in time was for all voters, so that because there were not enough accessible voting booths, that that's where it bottlenecked, right, that because there was going to be, you know, only one accessible voting and that was taking them so long to get through, that that's where the line was going to stop. So, you know, imagine you have 10 people online and everybody's moving through with the check-in process. But you cannot check in more people than can vote, right, so that's where the stall happens, right, is that just because, you know, the line is going to start at that first stop, right? So if you have a three-hour wait line, you can continue to check in those voters, but they're not going anywhere, and so, like, that's where the stop would happen. So that's what it's visualizing. And if that's not clear, we can touch base afterwards. Yeah.

MS. GOLDEN:

Diane Golden. And this is just a question coming from someplace where there's some really small jurisdictions. Is there any warning or flag on those that are going to come out legitimately

with one legitimately? It's a small jurisdiction, and even if you use a 20 percent, you know, disability prevalence rate, you're still probably going to be at one. The caution of if that accessible machine produces a ballot that is fundamentally different from the one everybody else is using because everybody else is hand marking usually, and it's a different size, shape is readily identifiable, you are going to have to have other people vote on it than people with disabilities who request it, or you're not going to have a secret ballot any longer, you know? Is there any way for the system to flag that, remind people if they're going to use it and they're at the smaller end of the scale? That's the secondary issue that's not just about numbers. It's about privacy of the cast ballot.

MR. JACKSON:

Certainly. And so that was an issue that we ran into in Maryland that hand marks and uses the ES&S paper ballot is trying to, you know, ensure the secret ballot, that if you have one voter who is using an accessible machine, and you have a precinct of 300 voters, like you have a good to fair chance of, you know, possibly identifying whose vote that was. That's something that we can add into the instructions to say that, you know, besides the fact of, you know, wait time optimization, that another, you know, second-order impact is like ensuring the privacy of the ballot. But

there is not a current flag, but I think that is, you know, a fantastic point and something that can be added.

MS. GOLDEN:

And, honestly, maybe the suggestion is making sure people know it isn't really just for people with disabilities. I mean, you know, anybody can use it, even if they don't look like they have a disability to you, you know? They might, kind of that. It's -- yeah.

MR. JACKSON:

Yeah, certainly language like instructions, which Maryland change was it went from hey, do you want to use the accessible voting machine to, hey, do you want to use the electronic voting system? And that did increase the number of people that used it.

But yes, in addition to that, language access is probably another population that could take advantage of this, and so you can start with your minimum of like roughly 16 percent of voting age population in counties across the country have a disability, but then in those other designated, you can add another two-plus percentage of either low English proficiency or people whose English is not a first language if the systems are programmed in other language.

So yeah, there are a number of different uses for the accessible voting systems and so, yeah, there's, you know, definitely making sure that anybody who wants to use it can use it

and is not thinking that is solely for a designated population, so, you know, reducing or eliminating that stigma is something that I think is very important.

MS. WATTERS:

All right.

CHAIRMAN HOVLAND:

Well, Ben, thank you for the presentation. And, like I said, glad to get that on the front side of lunch, so maybe we can help some people avoid traffic a little later this afternoon. But that does bring us to our lunch break of the day. For folks on the TGDC, we've got you covered, so just hang out. For other folks who are here, lunch is on your own. Good luck out there.

[Laughter]

CHAIRMAN HOVLAND:

But we will resume at 12:45. So for anyone just looking for a brisk walk outside, you're also welcome to do that, but we will be back here in an hour. Thank you.

MS. CHILDERS:

And if you need any recommendations for lunch options nearby, there is a list up on this table right here. Thank you.

[Recess 11:49 – 12:50pm]

MS. CHILDERS:

Okay. All right. Thank you, ladies and gentlemen, for coming back. I hope you had a lovely lunch. We're going to do some quick housekeeping notes here. Our captioner has requested that if you are talking into a microphone, that you identify yourself at the beginning of when you're speaking, which I did not do just now. So I will say I am Monica Childers, and that will help him to actually put correct captions up there. So thank you very much.

And to our presenters for this afternoon, thank you so much for presenting. You will have me timing you, and I will show you signs as you're getting close to the end of your presentation to try and keep us on time. Thank you so much, and I'll hand it back to our DFO.

CHAIRMAN HOVLAND:

Thank you. Ben Hovland. I'm glad that housekeeping matter reminded me to do it as well.

Welcome back. I hope everybody had a wonderful lunch. And so to kick off our post-lunch, if you're following along with your agenda, again, we heard from Ben Jackson before lunch, and now we are moving on. We're going to hear about the EAC Field Services effort, so we're going to welcome back Brooke Watters.

MS. WATTERS:

Thank you very much. Good afternoon, everyone. I am Brooke Watters, again, the acting Testing and Certification director for the EAC. Field Services falls under Testing and Certification, and I have the privilege to do a case study with you about some of what they've been doing.

I did want to note that the Field Services Program really comes from the Quality Monitoring Program piece of Testing and Certification, which we've had in our program for a long time, and the purpose of which is to ensure fielded systems are identical to those fielded are tested and certified by the EAC. We monitor for completeness and adequacy of testing with desired performance in fielded voting systems and monitor the effectiveness of the VVSG.

Field Services does more than that, and I'll really get into it, but they are a critical piece. Outlined in chapter 8, section 2 is the purpose here. And, historically, we have been a little resource-constrained with being able to do these efforts. But now we have a team of six led by Dan Cox, the Field Services program manager, and his team, who's divided up the territories into an LLC map with all five regions being covered.

So to go over the case study, we've chosen to look at the Douglas County, Nebraska, case. I'm making sure it stays on this slide. Sorry. So with this case, even though we've already -- as we were getting established with the Field Services Program team and

had done some onsite observations, as well some communications with other states and localities, this one was really kind of our first bigger project. It's often called the pilot because it had the full effort here where we went from the federal level to the state level to get the state involved and make sure that they are looped in at every stage. They were actually interested in potentially doing a statewide rollout but knew that that would be a very large undertaking. So, instead, they asked to do a pilot program looking at one of their counties, and they recommended Douglas County.

Douglas County also uses ES&S's EVS 6.1.1.0, and so the manufacturer, ES&S, was also looped into this effort. And so, following the proper order of operations here, we went from federal to state, state to locality, and then reached out to the vendor for that extra support as we did these efforts. I'm just making sure I'm not missing a piece here. My apologies.

From our team -- and this is nice. We have this little picture up in the corner from our team. The individuals onsite were Dan Cox, our program manager, as well as Roger Piha-Paul, who is a field service specialist. He has region 2, including Nebraska. A lot of effort went into the communication pieces here on making sure that everyone was on the same page.

So following the trajectory that we have on screen here, a lot of this actually comes from the outreach that we did initially. So as

Field Services was coming online, they performed a lot of outreach to the different states and gauging their interests in participating in something like this.

We do a lot of other things with Field Services, whether that's answering questions or providing trusted hashes, but effectively, we would love to see more onsite efforts like this, but we are a voluntary program, and we are not just going to come in and say we're doing this. We need to make sure that this is something that the states and the localities want done, and we're going to do it at their comfort level. Ultimately, it is feeding back into us, and we're learning a lot from here, but it needs to be good for everyone involved.

So after we did our initial outreach, working with the state and the county, we put together a scope of what this would look like, which involved planning, the processes and procedures, the participants on who would do what. A piece of checking these systems is to perform hash verification and using our trusted hashes, as well as the scope of conformance that was issued by the EAC for these systems, and then observing this whole process. And I'll go into that in just a minute.

And then every time we've gone onsite, whether it's a bigger effort like this or a smaller one, we're putting together mostly an

internal document for ourselves, but something that the state could potentially use as well with a drafted report that could be published.

Again, just making sure I'm not missing anything. And actually, I can leave it here, unless you would like to see that graphic, but effectively, I want to go into what that scope looked like.

So everyone had a really important role to play here. So the Secretary of State's office was actually the ones that initiated that conversation with Douglas County. The Secretary of State's office also provided laptops and in-person IT personnel to help with these efforts. The county provided staff, both staff to participate in this effort, but as well as staff to also observe and be trained on these efforts. Often, we see with election officials, there can be a high turnover rate, and even if there's not, the individuals coming in might be very unfamiliar with how an election works, right? There's so many other aspects to their job that they're just unfamiliar, and so having something like this, being able to get them up to speed is very valuable.

And then we had ES&S onsite as well to answer questions. They had an arm's length role where they were just also considered observers, but the experts in their own systems in case something were to come up, like a question on how are these procedures being done.

For the comfort level of everyone involved, it was agreed upon to look at the central scanners for the entire county, as well as a sample of all BMDs and, ultimately, the configuration onsite met the scope of conformance that was issued by the EAC and no additional issues found. The system was identical to that that was tested and certified.

So, ultimately, case studies like this, projects like this are very valuable. They're successful projects. Even if something is found or not found, ultimately, we have created this conversation, this communication piece that has been kind of not completely there in the past. We're closing this feedback loop and getting information.

And it can be a little bit different for all states and localities. We've outreached, and 34 out of the 55 states and territories have expressed interest and are looking to participate in this program, and we're already working on efforts for this year of 2025 in creating a list on where we can spend our efforts because even though we have a dedicated team, a team of six, that does not mean that we can handle all 34 of these at once. We're still not there yet, but we're able to go in the right direction.

Some jurisdictions actually rely very heavily on vendors, and it's helpful to bring them into this conversation as well. We're not looking to exclude anyone here. We're looking to have a very

complete conversation. And, ultimately, while we're looking to help the election officials verify their systems, they're also helping us out because the piece and the purpose is we are checking the effectiveness of the VVSG, and this is one of those feedback points that we're doing with stakeholders as we do our annual review. A lot of this information is coming back to us, whether it has to do with testing and how our test labs are operating, or how the requirements are being met, or what some of the difficulties are being faced on the ground level. This information is highly valuable. And, ultimately, the collaboration is exactly where we need to be.

So this was very brief. We have some other samples that we've done out in the field, and I know that we have Sean Pumphrey in the back here, who is one of our election technology specialists, and next to him is Dan Cox, the program manager, and they will happily talk your ear off about any of these other projects that they've either done or are looking to do.

But to keep it brief, as I'm sharing this time with another case study, are there any questions?

MR. WLASCHIN:

Chris Wlaschin, I am here representing ES&S and many of the registered manufacturers in the EAC program.

I applaud the EAC and the Field Services team for undertaking this effort. This effort helps answer that big question that many election officials get every cycle asking, how do we know the machines are still in the approved configuration? How do we know that they're still set up under the design specifications? How do we know that they remain reliable? Well, the EAC Field Services team undertook this head on. You mentioned a lot of collaboration, and there absolutely was. I believe it's necessary to accomplish this. Keeping the manufacturer at arm's length is a smart thing to do. It addresses that concern that somehow manufacturers are attempting to subvert the results. Why we would ever want to do that, I don't know, but people say that sometimes.

We have had other manufacturers now ask us about the experience. How did it go? What's the right timing? I probably wouldn't have wanted it to be done just a few months before a presidential election, but that's the product of Wayne Bena at the Secretary of State's office raising his hand. If you know Wayne, he does that a lot.

But it worked. I thought the pilot worked to perfection and helped us understand more deeply what the Field Services initiative is about and that we are recommending it to our peer manufacturers as yet another independent verification that the EAC and the VVSG is working.

MS. WATTERS:

Great. Thank you.

MR. CASKEY:

Brian Caskey from NASED. Could you go into a little bit more detail on exactly what the program did? Like I'm assuming that no one touched any of the machines, and so can you go into a little bit more detail on what exactly what your team did and how that looked on the ground?

MS. WATTERS:

Sure. Just for time sake, I'll be a little brief with this. But still, our team is there to observe. We have a whole learning library of best practices and documents that our other divisions like clearinghouse and grants work on, and we have that intimate knowledge with it. So onsite, we're here to really talk through what the process looks like. A lot of states and localities aren't regularly going through a process where they're checking their systems, and so what we're doing is we're kind of walking them through what that looks like, but we're not touching their systems. So it's a lot of -- training could be the word here, but it's really just informational assistance, and then that also feeds back into our program in a positive manner.

So some of what that is is they're not even sure where to start, so we help them with picking out, well, what parts of your

system are we looking at? Some counties are so large you can't look at every single device, so what does it mean to take a sample set? And what's the time frame that we're doing this in? And part of logic and accuracy are risk-limiting audits. And those have been conversations that have been brought up, too, to have the EAC onsite to just kind of help with double checking that the best practices are being followed in these cases.

Yes?

COMMISSIONER PALMER:

Commissioner Palmer. Could you describe the problem a little bit? I mean, you know, we would travel and there would be localities that are having issues with the tools for hash validation. There were some issues where the hash, for whatever reason, didn't match. So some of these issues were out there. Could you explain how this program can help sort of raise the level of technical proficiency in counties providing and doing this test?

MS. WATTERS:

I think so. Our ground team might have a little bit more insight than I do, and I'm sure that they'd be happy to continue this conversation. But, effectively, being able to go onsite if something is reported that it's not matching or we're finding it, it's often with the procedure not being followed closely, or there's just a confusing piece here that, because this isn't being done widely on a regular

basis, we're finding that we are taking this information back into the program and getting things updated, getting some systems updated to have consistent procedures that are being followed.

So even when there does seem to be a finding, it really is still a positive insight, and it doesn't mean that the system is not the same certified system that we've tested here at the EAC, but it's simply that we're getting there. This is a baby step in the right direction of making sure that what is fielded is the same.

I know I'm not fully answering the question here, but it is helpful to at least start this discussion and figure out, well, where is this coming from? Because we have seen instances where you type in the wrong thing when doing the check, the matching check because these hashes are long numbers and characters, as well as many files that are on the systems. And there's a lot to undergo and take on here, so there's bound to be a bit of a learning curve involved. And mostly what we're seeing is just helping get through that learning curve.

COMMISSIONER PALMER:

Just a brief follow-up. Where is the report? Is it on the website where folks can read it?

MS. WATTERS:

So I believe we have published. Right? I was going to say, hand it back to Dan.

COMMISSIONER HICKS:

I was about to say, Dan, come up and answer some of these questions.

[Laughter]

MS. WATTERS:

These are recent. All of this feedback is coming in and might be considered a little bit more internal because it's feeding into the VVSG, but for the Douglas County pilot, we do have a report that, if it's not already published, it will be soon.

But, Dan --

MR. COX:

Should I take the podium with you? I'll stand next to you.

MS. WATTERS:

That works.

CHAIRMAN HOVLAND:

Dan, come on down.

MR. COX:

Hello, everyone. I'm Dan Cox, the Field Services program manager. So, Commissioner Palmer, to answer your question, is it published to the website? It will be in the coming days, actually. And one of our other pilot projects with the State of Hawaii is currently published as we speak on the Field Services reports page, so happy to share that. Got it.

MR. SKOGLUND:

Kevin Skoglund representing IEEE. So it's fantastic that you guys are doing this and that you're gathering this data. I'm a firm believer that what gets measured gets managed. I'm wondering, though, specifically about VVSG, are there things that you have found that you think need to be addressed in some way in the VVSG or there could be improvements that would facilitate this and make it better?

MS. WATTERS:

So far, I would say that there hasn't necessarily been something confounding about this requirement needs to be updated today but might be something that needs to take a little bit closer look at and making sure that our labs are doing a full evaluation check. We do have the opportunity with our Field Services team to not be limited to just EAC-certified systems. If the state and locality are interested, and it is not an EAC-certified system, it's typically a similar baseline and a similar set of procedures for going on and doing these best practices.

So some information is, how state systems varied from EAC systems, and that has helped us with the testing side of the program, though they haven't necessarily played a role into here's a requirement that needs updating, at least not yet.

COMMISSIONER HICKS:

Well, since I haven't spoken today, I guess I should speak at some point so folks know I'm actually here.

MALE SPEAKER:

Who are you?

[Laughter]

COMMISSIONER HICKS:

Tom Hicks, Commissioner with the U.S. Election Assistance Commission, who will celebrate his 10th anniversary with the agency tomorrow.

[Applause]

COMMISSIONER HICKS:

And, as Monica would say, always making it about himself.

[Laughter]

COMMISSIONER HICKS:

So, Dan, I was able to participate in the service that you've provided to the 50th state, and one of the things that I thought was fascinating was that they were willing to hear some of the recommendations that you were going to make as you were going through this, and so not necessarily all about machines, but one of the things being chain of custody and things like that as well.

And this goes to what Brian was saying. We're not going into a state unwelcomed. We're being invited into it, but also just going in and how can we offer improvements? It doesn't mean that

these things have to be taken or they might be looked at in a different way, but it's more of, how can we, as the EAC, look towards making the systems better? That's all.

MS. WATTERS:

Great. Thank you. All right. Thank you, everyone.

CHAIRMAN HOVLAND:

Well, thank you. Thank you, Brooke, and thank you, Dan and Field Services.

I will just say we wanted to provide this update. I know last year at this meeting, we did a little bit of a preview, and so a nice follow-up now that we've seen some of these pilot efforts, again, as Brooke highlighted, this is something that we not honestly have the historic resourcing to fulfill that part of the Testing and Certification Manual, so we're excited to see that.

But it is an evolving process. It is one where we learn, again, recognizing 50 states, five territories, the District of Columbia, and over 8,000 jurisdictions, we realize that six people do not do that overnight, but it has certainly been a learning process. It has been services that we can provide at the EAC. We certainly look for ways to scale and scope portions of that, but it is also informative to the overall process and having some of those contacts we also know can be useful for things like anomaly

reporting and other broader benefits to the program. So we're excited about that progress and to continue that.

Next up, we're going to hear from the Election Supporting Technology Evaluation Program, again, another newer program in the scope of the EAC, but recognizing that there is more and more election technology that falls outside of the scope of the Voluntary Voting System Guidelines. But nonetheless, there is a need to support election officials and jurisdictions on that.

So Jay Phelps and Liz Beatrice, if you all could come up. Oh, great. There you are. Take it away.

MR. PHELPS:

Good afternoon. Thank you, Commissioner Hovland. Thank you, NIST, for hosting, and thanks to everyone for being here. I see a lot of white snow out our window here, and I left Indiana with about 18 inches of snow, so certainly understand kind of what everyone's going through who lives here and in Baltimore, Maryland.

For those who don't know me, my name is Jay Phelps. I am the director of the Election Supporting Technology Evaluation Program, or ESTEP for short, like we like to call it. And I'm here with my colleague, Liz Beatrice, and we're going to give you an overview of where we are with the KNOWiNK test campaign. But first, I wanted to kind of back up and let you know where we've

been in 2024 and where we're going to go in 2025, and then we'll answer some questions at the end.

So for, you know, 2024 accomplishments, 2023 was a year of growth, of hiring our team, our election technology specialists. Running through the pilots, we had several participants, as you might be familiar with, and taking just all of our stakeholder feedback from our FACA boards, from NASS, from NASED, the recommendations from NIST, and building the electronic certification program into what it is today, and that would not be possible without the feedback and the input from you all, from our stakeholders, from our election officials.

So I just want to say, first and foremost, thank you for your valuable time, for your input. We still have a lot of work to do. We still have a lot of refinement in the future as these technologies continue to rapidly evolve, but we certainly want to partner and have you be a part of that with us.

In April of 2024, the Commissioners approved not only our ESTEP manual that put forth the guidance for our program but voted to certify our Electronic Pollbook Certification Program. And six, seven weeks later, we received our first manufacturer registration application, as well as application for testing by KNOWiNK, and so we accepted that in June of 2024.

And one thing just to note, statewide electronic pollbook test campaigns versus our federally certified Electronic Pollbook Certification Program, we do have usability testing on our side, as well as penetration testing and enhanced requirements across the board from functionality, security, and accessibility. So it does look different.

But one of the things that we were able to do during the pilot and even before the process as we're developing our electronic pollbook requirements is to look at states to lay that groundwork, like Ohio and Indiana, and talk with other folks like California and New York. So that was really helpful.

And then, most recently, in 2024 we released requirements for feedback. So the next pilot in queue is our Voluntary Electronic Ballot Delivery Program. I'll get used to that one next. We have a set of requirements, hundreds of hours research going into that, working in partnership with NIST. They provided a lot of valuable feedback and input last summer. We also ran those requirements through our FACA board. So those of you in this room that provided feedback, thank you so much for your input.

Due to the presidential election last year, we decided to wait until after the election and the holidays to send those to NASS and NASED, so we did send those to NASED on January the 3rd for a

60-day review that ends on March the 4th. So thank you for everyone who's reviewed and just taking the time out to do that.

The next pilot that we're going to kind of simultaneously kind of piggyback, so to speak, is our Voluntary Election Night Reporting Pilot Program. Same thing with the requirements, we had NIST review last year on a 60-day review, and because of the election, we paused not only the NASS and NASED said review but the FACA board review.

So you might have received an email, for those sitting around the table, from Monica Childers -- Monica, thank you for sending those out -- on Friday for a 60-day review. I understand you probably haven't had time to review those. That was not an expectation. However, in the coming weeks, if you could just please take a moment and review those and give us valuable, critical feedback. That's why we send those out. That's what we want from each of you. What are we missing? You know, look at it from obviously an expert, but also a user, right? Where's our limitations? What could be some, you know, problematic requirements? We want to hear that feedback from you.

So, again, when you get a chance, please review those. There is a contact. Jen Day is our Voluntary Election Night Reporting contact for that, so her contact is in that email. You can always, of course, contact me anytime as well. Please see me.

I've got a business card with my contact information as well. It'll be here at the end of the presentation also and would love to talk anything ESTEP-related, so I want to be sure I put a plug in with that. And then, of course, NASS and NASED we also sent those out here on January the 6th through the March the 4th, kind of having the simultaneous window for feedback with those.

So where are we going? I think 2025 is going to be a very ambitious year for ESTEP, especially with no federal election, and we hope to launch three pilot programs, definitely at least two of them with, as I just spoke to, Voluntary Electronic Ballot Delivery pilot. We hope to launch that in April, our Election Night Reporting pilot in possibly June. Again, these are all tentative time frames based upon feedback, based upon all the responses received and going through the formalized process.

And then for our Voluntary Voter Registration Systems pilot, chapter 3 of our ESTEP manual gives us the opportunity, through the technology testing agreement, to reach out to, you know, stakeholders as well as manufacturers and just have conversations about their systems, where they're at, limitations, the user experience. And we did that with our electronic -- and, of course, this is in conjunction with the Public Records Act, so we did clarify that.

But with our Voluntary Electronic Ballot Delivery and Election Night Reporting, we did the exact same thing, meeting with these stakeholders to help build out our requirements. So sometimes folks are like, well, where do these requirements come from, or how did you get some of these ideas? And it's honestly from you all and just listening and communicating and having that open experience.

So, currently, through this month and next month, we are meeting with some of our stakeholders and manufacturers. I know the State of Nevada is one, as well as North Carolina and a few other manufacturers, so we're looking forward to that, just that information-gathering session, and then we'll go through the similar process, right, where NIST has given us baseline recommendations, and we'll have them do another review, and then we'll open it up to the FACA boards, NASS, and NASED, and probably later on in March for a 60-day review period. So just wanted to bring that to everyone's attention.

And then one thing that needs to be said is, you know, with electronic pollbooks, this is something even before I was hired that the Commissioners have been talking about. And they've heard from stakeholders we need a formalized program. We need standards in place. So there's obviously statewide examples of what a program looks like.

Both these other three technologies that I just mentioned, the pilot is going to inform the future of those, right? Maybe it's best practice if our pilot experience tells us something different. Maybe it's a white paper. Maybe it's requirements, best practices the states can utilize and what's best for them. We don't know. That's why we go through this pilot experience as a factfinding and data-gathering experience. So I just wanted to mention that as well.

And then, finally, before I turn it over to Liz, at the end of this month, we are going to be publishing on our website under the ESTEP portion some election-supporting technology logic and accuracy testing checklists for stakeholders to be able to utilize before each election for these technologies and things that they -- it's very baseline so it can be utilized across jurisdictions. But it's basically, you know, have I made sure that my electronic pollbook -- talked with my manufacturer to be sure the most up-to-date version has been installed, no check-ins on it, basic things like that. And so be looking for that published at the end of this month.

And with that, I am going to turn it over to Elizabeth Beatrice. To give a quick bio of Liz, she comes to us from the Voting System Technical Oversight Program where she was program manager. She's been with the ESTEP team for about 18 months. We're very

lucky to have her. She's done a great job leading the Electronic Pollbook Program. So, Liz, I will turn it over to you.

MS. BEATRICE:

Thank you, Jay, and thank you to everybody for having me here today to present to you on an exciting new initiative at the EAC. I'm typically nervous when I start presentations, so I try to find a joke, and I will apologize in advance that I researched this one with ChatGPT --

[Laughter]

MS. BEATRICE:

-- so if it's not funny, I do apologize. Why do electronic pollbooks get invited to every election? Well, it's because they want to make sure they can count on a good time.

[Laughter]

MS. BEATRICE:

All right. I apologize in advance.

As Jay mentioned, I do come from VSTOP originally, where I did work with electronic pollbook certification there in the State of Indiana, and I've been with EAC -- I can't believe it's been 18 months; that's amazing -- working primarily on the electronic pollbook certification program at the EAC now.

So before I get into the intricate details of KNOWiNK's certification, I wanted to talk a little bit about what our certification

process looks like. It's very similar to the testing and certification process for voting systems, and it follows a general eight-step process.

First, the manufacturer is required to register and submit an application package, and then it will transfer to the jurisdiction of the test lab. The test lab will do a test readiness review and penetration testing simultaneously, but they are different processes. And then once all of that process has been done, they will do a test plan and let the EAC know that the system is ready for testing.

Then the actual test execution begins. So, as you can see, the five-step process before test execution is kind of different than the state certification process. It's a little bit more involved to make sure the manufacturer is actually ready and prepared to enter our program.

And then after test execution, the test lab will issue a test report outlining the findings of the process. And, as a matter of fact, the test report won't get issued until they've had a long conversation with the EAC making sure that every single requirement has been met. And then lastly, we will decide to grant or deny certification, and we should always grant certification after we've received that test report.

As I did mention, there are two prerequisites for manufacturers. These are the manufacturer registration and the

application for participation form. The purpose is to make initial contact with the EAC, provide general information about the organization and the system for testing, and then agree to the program's procedural requirements.

The application includes the technical documentation package, as well as the system for testing. And then the technical documentation package includes listing of accessibility capabilities, the device's capacities and limitations, the system's coding convention, the functional diagrams for the system, a list of the client jurisdictions, and the training materials for the system, as well as any other documentation that is required in the e-pollbook requirements. ESTEP approval is required before testing begins on both of these forms.

We do have a three-tiered approach to testing through functionality, security, and accessibility. Combined, these make up 110 total requirements for certification. Functionality is a new section that was added as a result of the pilot. This includes testing for usability, the system's configuration, its overall compatibility, and the ability to communicate with voter registration if that feature is available, and then just baseline maintenance and troubleshooting.

Security focuses on access control, physical security of the system, the system's overall integrity, the network security, the

software design and architecture, and the supply chain risk management.

And then, lastly, with accessibility, we want to focus on the baseline accessibility requirements kind of required under section 508, and WCAG. This will also look at visual features, physical features, audio features, and the system's ability to support additional languages.

I will say also that all requirements must be met to achieve federal certification, and we do have some requirements listed as if applicable. Those are not intended to be synonymous with optional. If the functionality is supported, it must be tested.

And now to the exciting part of KNOWiNK's system that was submitted for testing. They submitted the Poll Pad version 3.6, and this was evaluated by SLI Compliance. We are currently under phase 7 of 8, which is the test report, and we actually received an exciting update yesterday that we should receive that by the end of this week, so we'll probably be moving to phase 8 at the beginning of next week.

We did learn a few lessons, as we will with every test campaign, and there are four that I wanted to highlight for you today. First, that weekly progress check-ins are necessary for success. We actually implemented these early on in the test campaign as a result of the pilot program because the pilot dictated

that manufacturers wanted to have more interaction with the EAC. And we implemented these early on in the kickoff phase, and we'll continue to do that in future test campaigns as well.

Second, clear expectations must be communicated before application package approval. Manufacturers should always be prepared to meet our requirements. This will result in greater efficiency and fewer questions and fewer delays.

Third is pretty self-explanatory. Manufacturers will need to rely on the EAC and test lab support during the test campaign to be successful.

And then, lastly, we did find an interesting finding. Outcomes will vary between pilot and certification testing due to a variety of factors. Once you hear the explanation, it kind of makes sense. Maybe a manufacturer submitted a new system or new components for testing that they didn't submit in the pilot, or, also, they could have submitted the same system without looking at our updated requirements.

And, lastly, we do have a few plan improvements that we are working toward for the next round of testing. Particularly, those are to revise the ESTEP's manual and the e-pollbook requirements. These are only a few of the recommendations we have at this time. First is to clearly define the eight-step certification process. Second is to update the language for minor changes and modifications to

allow for greater efficiency in our program. And this will also be similar to Testing and Cert's process, as Brooke mentioned earlier, hoping for a three-day review process on minor changes. And then, lastly, we do want to require 508 compliance for all materials submitted by manufacturers and test labs, which is basically just to ensure that all materials posted on our website will be accessible to the public.

And then, lastly, we do want to look at e-pollbook certification requirements again. We are considering revising the language for usability testing expectations. The current expectations require a third-party test lab to review all the materials submitted by the manufacturer to make sure that the system is actually usable by a different variety of people. This has very minimal oversight by the EAC and the test lab, and we just want to make sure we can expand that oversight in the future. Additionally, it incurs additional testing costs for the manufacturer. We're hoping to have more test lab involvement to limit that additional cost.

And then not listed here, I wanted to also mention that we're working with the EAC's accessibility workgroup to prepare manufacturers for ADA title II requirements since those will be required by states in 2026 and 2027 for localities.

If there are no questions, there is a QR code on the screen if you're interested in learning more. You can also visit EAC.gov and

look at the election technology tab. And then here is our contact information.

And then I think last we have just questions. So are there any questions? And I'll invite Jay to come up and answer those with me.

COMMISSIONER PALMER:

So this is a question sort of from the audience that I got during the break. So the first question is, actually under functionality you talked about the connectivity with the cloud or with statewide -- how far do we evaluate or test that security or functionality? Because I know it's somewhat connected to the VR system. And so that's the first question.

The second question is, so now we've had a vendor go through this process. You know, we did have a hearing, and there was a lot of interest in the pilot. We had a number of vendors work in the pilot. And so where do you think we go from here with the other manufacturers and vendors?

MS. BEATRICE:

To answer your first question, as far as any network security for connection to voter registration systems, that is evaluated if the system supports that functionality. So what we'll do is have the test lab security teams, A, run a penetration test on that before the actual test execution begins so that that will already be technically

pre-evaluated before we even get to the test execution phase. And then, secondly, they'll go through -- I believe there's multiple requirements that address network security in our e-pollbook requirements, and I could pinpoint those exact ones once I get back to my computer.

Jay, did you want to answer the second question?

MR. PHELPS:

Yeah. As far as your second question, Commissioner Palmer, you know, I think where do we go from here? Like Liz mentioned -- and there's quite a bit of other things that we internally can improve up on. But I think socializing kind of the experience both from the EAC's perspective, but also on the manufacturer to, you know, talk with our stakeholders about how this process went, why it's valuable.

I think, you know, in the last, you know, six months, three months especially, we've kind of had our heads down working on this campaign. But I think, you know, kind of hourly facing now that the election is over, letting folks know the benefit, also, you know, the potential cost savings as well for a state to be able to go through our program.

And then third is to look at, you know, states utilizing our, you know, mandating requirements in their state legislation as far as going through the EAC in the future and why that could be

beneficial. I believe the State of North Carolina is one that is looking at adopting our electronic pollbook standards, and so we look forward to talking to them further about that.

And so I think those are just a few things that we can do as an agency but continue to increase communication with our stakeholders across the country to let them know exactly what we're trying to do here and how this has been official, and, if nothing else, provide recommendations for them. If they're a little bit -- you know, if they already have a statewide program, how can we assist them with that statewide program? What's some things that we could add, too, to enhance that I think is really important to look at.

CHAIRMAN HOVLAND:

Well, hearing no other -- Diane, go for it. Yeah.

MS. GOLDEN:

This is just a quick follow-up. So there's an accessibility work group somewhere.

MS. BEATRICE:

Yeah, it's just internal to the EAC, composed of a few different experts on the agency with accessibility.

MS. GOLDEN:

Okay. Thank you. And just a question about, so these are the same test labs doing VVSG certification that are doing all of this

extra stuff. What's happened in terms of getting staff within those entities up to speed on certification to WCAG? Because that's a bit of a different beast from what they've been doing with the VVSG. I know it's in there, but, yeah, it is really a totally different -- yeah, can you just -- or can you talk me through the protocols they're using, and whose model did they pick up on to do WCAG conformance testing, which is as much an art as a science? Anyway, I'm just trying to get a feel for how they upscaled to be able to do this appropriately.

MS. BEATRICE:

That's a great question. We actually have worked with the Testing and Certification Program to make sure that the labs are equipped and ready to test to the e-pollbook requirements version 1.0. And they're actually going to be updating their accreditation certificate to include that in the scope. And, as a part of that, we actually do require that the labs have test cases specifically for each part of the e-pollbook requirements, one of those being the accessibility test cases as well.

The test cases for e-pollbook accessibility requirements have been developed based on the -- I can't remember what the acronym spells, but it's the VPAT developed by the W3C, which created the WCAG. And that's the extent to this time, but we do

encourage any recommendations to improve that process in the future. The testing teams as well also have accessibility experts.

MS. GOLDEN:

Okay. Diane Golden. There's a bit to unpack there. So test cases to me are, you know, a person test case, not -- so the VPAT, the Voluntary Product Accessibility Template, is literally the WCAG 2.0 requirements. You know, cursor focus must X, Y, Z. You know, tables must do this or not do this, or, you know, headers and nesting, and I'm just throwing out terms because that's about as much as I understand it because I'm not a coder. That's totally different from a test case person type testing.

And, again, I think what I'm looking for is like so if the test labs required -- and I can't even come up with the credential now, the certification, the accessibility IA whatever, there's some credential out there now that is basically web accessibility conformance understanding, there's different levels, have they hired those kind of credentialed people? Have they beefed up that part? Is that what's happening?

MS. BEATRICE:

I do believe they do have accessibility-specific testers on their team, similar to penetration testing. They have those fields that they've been accredited and certified in specifically for those kind of groups if that makes sense.

MR. PHELPS:

I'm going to just add one other thing.

MS. BEATRICE:

Yeah.

MR. PHELPS:

And one other thing I will add, Diane, and this is an idea that we're thinking about as an agency with the adoption of ESTEP and these rapidly changing technologies is the possibility of what happens if we have a manufacturer that does not have a voting system but would like to come through our program to test? What does that look like? And so we're thinking about creative, outside-the-box ways of thinking with a potential kind of -- if there's an organization that can test just the accessibility portion of our requirements, for example, in the future, what would that look like versus someone who has, you know, security experience and kind offer kind of that piecemeal? Again, that's an idea, Commissioners, we're just exploring.

But to your point, we have talked to both labs, you know, extensively regarding our current, you know, requirements for e-pollbooks and also the future, you know, technologies to make sure we're staying in communication with any changes because, as you can imagine, you know, yes, they kind of understand what we're

thinking with these other technologies currently, but they're going to change until we really get past the post-pilot phase.

CHAIRMAN HOVLAND:

Well, thank you, Jay and Liz. I think one thing that I think is very cool about this or that I like, obviously, for you all, for the TGDC, this is outside of the scope of the primary focus of the VVSG, which is the primary focus of this body, but I think that one of the great things about ESTEP is that it has a little bit more flexibility. It has a little bit more -- you know, it can be a little bit nimbler. But we've also been working within the EAC to ensure that, you know, the silos are not too significant. And I think our work in this area can inform testing and cert. I think testing insert certainly informs the work in this area.

But much as, you know, those sort of jurisdictional lines don't apply out in the field for election officials, you know, they have voting systems, they have e-pollbooks, they have other election technologies, it has been useful to have this added emphasis within the agency to build out our broader program.

And so, again, great work by the ESTEP team. Thanks, Jay and Liz, again for the presentation, and we're excited to see the continued pilots moving forward and the near certification here of our first e-pollbook, which is exciting to have that on the horizon, so thank you again.

MR. PHELPS:

Thank you.

MS. BEATRICE:

Thank you.

MR. PHELPS:

Thank you for your time.

CHAIRMAN HOVLAND:

With that, we will move to our next panel, which is sort of a panel. I say sort of a panel because when I think of a panel, I often think of it as a table, which we don't have, so we will invite folks to come up one at a time, but certainly looking at another exciting conversation around end-to-end verifiable voting. For those of you who did not get enough math talk earlier or were really excited to be talking about FIPS, good news, we are going to go down the end-to-end cryptographic rabbit hole again.

So with that, I'd like to welcome Dan Wallach up. He's the program manager for the Information Innovation Office at DARPA, which I'm not going to attempt to spell out but Dan can, and also a distinguished former member of the Technical Guidelines Development Committee. So welcome back, Dan.

MR. WALLACH:

All right. Thank you very much. I'm actually one of many program managers in DARPA. I'm not the program manager. Boy, that was --

CHAIRMAN HOVLAND:

I was trying to give you a promotion.

MR. WALLACH:

That would be a busy gig.

So thank you all. It's a pleasure to be here today to come back and speak to the TGDC. For those of you who don't know me, I was, and kind of still am, a professor at Rice University. I've worked in computer security, and at DARPA I have a portfolio covering a variety of software resilience, legacy software updating type things that I'd love to tell you all about later.

But today, I've been asked to talk about, so what is end-to-end verifiability, really? And I initially wrote down an outline. I said, yeah, that looks like an hour and a half --

[Laughter]

MR. WALLACH:

-- and so this will be a little bit of a rush, but let's start.

A lot of the concepts come back to Josh Benaloh, who finished his Ph.D. in 1987 at Yale. And to give you some context, the 1980s, well, this was the first decade after the public invention of public key cryptography. And Benaloh said, hey, you know we

could use that. And he started working out how you might do cryptographic things to create election verifiable things.

I'm not going to attempt to wave my hands and do math, but the core observation was that you could process encrypted ballots in a way that you could provide strong proof about properties of them. What does that mean? I might prove that this particular -- if it's a 1-out-of-N election, I can prove to you that there's exactly zero or one selections selected, but you can't tell which one was the one that was selected. So that's a property that anybody looking at any encrypted ballot could know that it was well formed, as in not over-voted. So properties like that back in the '80s were an intellectual curiosity, but computers were kind of slow and chunky back then. They're not slow anymore, and so now we have the possibility to do some really interesting things.

In Monica's talk earlier, she introduced some of the basic vocabulary that end-to-end verifiable people use when they talk about these things. The two terms that I think are the most important are "counted as cast" and "cast as intended." "Counted as cast" means that when an election official publishes a tally at the end of the day, anybody can look at all of the encrypted ballots and reach the same conclusion, that these encrypted ballots imply this public total. And that's a property, again, that anybody looking at what's sometimes called the public bulletin board can then verify.

But the "cast as intended" property is a little bit more interesting because Ron Rivest has a talk where he jokes that "One of the problems is that people aren't computers." If I tell you, okay, think of a 4,000-bit random number. Okay. You're with me so far? And now please raise it to a 256-bit power. That's not something you can do in your head. You need a computer to help you.

And the gap between the human and the computer operating on behalf of the human creates an opportunity for hijinks, for what if the software in the computer is evil or just misguided or faulty? How do you mitigate against that risk? How do you make sure that the digital representation of your vote corresponds to the voter intent?

There have been a wide variety of approaches that people have come up with. Probably the easiest one to understand was, again, brought to us by Josh Benaloh, this time in 2006 and 7 when he published some papers on this topic. And we had the idea that we could challenge a voting machine in a way that if it cheated, we would catch it with certain probability. So, that way, a voting machine has a probability of being caught in the act, so now it becomes verifiable.

And other people thinking at the same time coalesced on this term that we now call software independence, that we want to be able to know that we have the correct election outcome, no

matter whether the software might have gone bad. Of course, if the software has gone bad and has produced bad outcomes, there's an interesting --we get into another set of vocabulary where we can wander down, which boils down to, can we recover or not? And this is, by the way, why everybody in the cryptographic world has decided they love paper because no matter what goes wrong in the computer, you still have dead trees, which are very difficult for foreign nation-state adversaries to tamper with remotely. I'm now in a position where I get to learn more about our foreign nation-state adversaries, which I can't talk about here, but anyway, they pretty much cannot change paper in a box. That's more challenging.

Okay. So when you want to put this all together, how do you do that? Well, we've talked about usability issues because that challenge step becomes something that a voter who doesn't want or need to know about it might trip over. One of the key things that, again, Josh Benaloh, when we were working on STAR-Vote in Austin with Dana DeBeauvoir in Travis County, we were trying to figure out how to manage a paper ballot and an electronic encryption system, a ballot marking device style system.

And Josh hit on the amazing idea that the physical motion of the paper from the voting machine to the ballot box or not to the ballot box is actually that challenge. So a voter who -- the procedure is analogous to a voter saying, whoops, you know, this is

not my intent. And in elections, we have procedures for that. It's called a spoiled ballot. The spoiled ballot process can be overloaded into a voting machine challenge process. And, of course, most voters don't even know that they can spoil their ballot, but it is part of a standard process, and that was the thing that we figured out we could use. That, to me, was the single best thing that came out of the STAR-Vote process, that and I really like Wasabi peas. Dana DeBeauvoir fed us nice munchies.

Anyway, other things people have worked on in more recent years that are very relevant to this are how do we do cryptographic encodings of complicated ballots like ranked choice voting? The math turns out to work really simply for 1 out of N. It works very well for approval voting, you know, pick any number. But once you start saying, here's my first choice, here's my second choice, here's my third choice, the math gets really complicated really quickly. So these are the kinds of properties that recent researchers have put a lot of time and effort into.

We also have had to learn to deal with some nontrivial attacks that don't exist in traditional elections. So there's an attack called a clash attack. I will describe it simply. Imagine that we have multiple voters that have identical preferences. I know, crazy, right? Well, what happens if the machine sees that voter 2 has the same preferences as voter 1 who's already voted? So then the

machine could give them a receipt for the prior voter's vote, and so now you have two receipts that point back to the same ciphertext, and that gives the machine an opportunity to emit an evil ciphertext.

These are the kinds of questions that somebody says, ah, yeah, okay, and then everything gets a little bit more complicated to mitigate against that risk. So these are the kinds of issues that we, the community, have been grappling with and improving on in the past decade really.

I was asked to also talk a little bit about ElectionGuard. So ElectionGuard, again, Josh Benaloh. There are other great cryptographers who've worked in this space. I got to give a shoutout to David Chaum as well. But, really, Josh Benaloh's name is woven throughout this history in a good way.

So in 2016, after that election, Microsoft decided they wanted to do something to help democracy, looking at R.C. Carter, who ended up in charge of the result of this. So Microsoft created the ElectionGuard project, and Josh Benaloh started writing down math in Microsoft Word, as one does, and people like me started turning his math into code. So ElectionGuard really is a distillation of everything that we knew written down in a nice document with a nice spec.

So what is ElectionGuard? At the bottom, it's the same math that I've been dancing around all this time. How do we encrypt

individual ones and zeros on the ballot? But also, ElectionGuard defined all the layers on top of this. ElectionGuard defined how do I compose a ballot out of these little cryptographic primitives? You know, how do I do hashing? How do I do the composition? What do the proofs look like? So ElectionGuard was the first time somebody tried to write all of that down in a spec that people could argue about, throw darts at, and improve, and that Microsoft was willing to hire and pay professional developers to turn into real functional code.

That showed up in three of the four pilots that were up here on the board earlier. Again, thank you, R.C., for helping organize and making all that happen. Making an actual, real-world pilot happen is an opportunity to learn all of these pesky usability things that may or may not crop up, and then that helps you further evolve the system.

Let's see. 10 minutes. One minute left?

So the last thing I want to mention briefly is that DARPA and the EAC have been jointly funding an interesting pilot project where it's called CAC vote, not the greatest name in the world. The common access card, every U.S. military person has one, and it's a cryptographic token and it's an ID card. And I fried mine last week by accident and couldn't log in, good times. But we're saying, how do you integrate that into an end-to-end encrypted voting system,

and how might you use that, in turn, to support overseas military voters to give them a better voting experience?

So this is ongoing research. I used to be a performer on it. Now I'm in charge of it, which is kind of interesting. We're doing this jointly with VotingWorks. And, fear not, no actual, real ballots are in any danger of being cast, but we're hoping to do a test pilot election, you know, with made-up candidates, that sort of thing, on an actual aircraft carrier really soon. And if we're lucky, it'll be at sea at the time, and we get to fly to the carrier and back.

But, joking names, it could be Vote on a Boat.

[Laughter]

MR. WALLACH:

It could be Removing Barriers from the Carriers.

[Laughter]

MR. WALLACH:

But the whole idea is we're trying to see how we can use this toolbox of technologies from the end-to-end verifiable world to help solve hard problems that we aren't doing well enough at and we can do better.

That's all the time I have. I'd love to take questions if we have time maybe.

MS. CHILDERS:

I think we're going to do combined questions at the end.

MR. WALLACH:

Combined questions. All right. Well, thank you all so much.

MS. CHILDERS:

Thanks, Dan.

CHAIRMAN HOVLAND:

Thank you, Dan.

And as we progress through this, again, please write down and save your questions. Our hope that our panelists will be kind enough to answer them all, but I think each of these presentations will build a little bit.

And so for our next one, we will hear from Steven Musick, the chief technology officer of Enhanced Voting. Again, a product that they work on falls outside of the scope of the VVSG but I think is important to inform our work and thinking around this and certainly adds to the end-to-end conversation. So welcome, Steven, and thank you.

MR. MUSICK:

I'm Steven Musick. I'm the Chief Technology Officer of Enhanced Voting, as he said. We are an election technology company. Our primary way of looking at this is we write software to help election administrators run their election to help solve their problems, right, make things easier.

As he said, we're not a voting system, right? So what we're going to talk about today, I'm hoping, can be distilled to have some relevance to voting systems. But, obviously, it's not going to be one to one, so just bear that in mind.

In particular, the project I'm going to talk about today is one of our products called Enhanced Ballot. It's our electronic ballot delivery product currently used in 12 full states and a bunch of counties across another handful of states. And, in particular, we did electronic return in three of those states. And I'm going to talk about how we got there and why because I think it's really, really relevant.

So just a brief, brief history lesson I'm sure many of us know is that we originally kind of decided there was a problem with absentee voting because when you go to request your paper ballot, you have to get it delivered to you. And if you are overseas and you're in the military, you have trouble getting that ballot, right? So we came up, you know, with UOCAVA and some of these things. We said, okay, we can deliver a ballot to them electronically, but it's otherwise the same thing as general absentee vote by mail, right? It holds all the same security promises we would otherwise have for people doing that in the States.

And it was really a short leap from there to say, you know, now that I have this electronic marking project, then I can apply

accessibility guidelines to it, and suddenly people in the disability community, people who are blind, for example, can use a device to not just dictate what they're voting to somebody else or have to go to a polling location, right? So now they have the opportunity really for the first time to vote by mail independently, right?

But it turns out that has some challenges, right? Because one of the things that we really run into is if you are a voter that is blind, great, you got your ballot electronically, you can fill it out online. That's all great. But now, how do you print it? Most people that are blind do not have a printer, right? Why would you? You then need help getting to a printer. You print it out, and you get a piece of paper that you can't read, so you don't even know if it printed the right thing. And then you're usually asked to sign something with your signature and everything else, and you don't know where to sign. You have to put it into an envelope. This is a whole process that is complicated for these people.

And so it turns out one of the really simple solutions here that people hopped on a while back was just, why can't I just use a computer to do the whole thing, right, return it electronically? And so I'm going to talk about that because we all know -- I'm not going to go into the risks of this. I'm sure everyone here is at least a little bit aware. We use paper ballots for good reasons, right? We don't

have everyone voting on their phone because there's a set of unsolved risks and challenges associated with that, right?

However, due to the fact that this subset of voters has no real alternative, right? If they cannot go to a polling place to vote, they -- now a majority of states have some form of electronic return period and have had for many years, right? A lot of times this is just email. This is just send this fax, as if people actually use fax machines anymore. It's usually just an email, to be honest. And so these states either pass regulations to require this, or a lot of times there's a court case involved, basically because these voters are claiming they are disenfranchised.

And so we originally set out as just an electronic ballot delivery platform saying we're just going to do what we know is secure, which is, we're going to print out a paper ballot for you, and you can mail it in yourself, right? And it quickly became apparent that these states are doing the electronic ballot return thing anyway, right? And so we ended up asking ourselves the question of, do we want to be perfect, right? Is perfect really the goal, or are we just trying to be better, right? We obviously want to strive for perfection, but it still is a step in the right direction to say that we are going to implement a better version of electronic return than what they're going to use either way, regardless of what we choose to do.

And so that's really the method we took. We said we're going to do the best we can with current technology. So this is how we ended up at end-to-end verifiability because this is one way of solving several, not all, but several of the challenges associated with electronic return, at least the security challenges.

So from there, one of the real statements that every software engineer knows, you're taught this really early, is, don't roll your own crypto, right? That generally means that this cryptography is written by a bunch of really smart people. It's really hard, it's really easy to make mistakes, so the average developer shouldn't be doing it. You should be using something in common that NIST and all these other people really know a lot about because they've got mathematicians and everything else on their side saying this has been tested and verified and all this good stuff. So we chose the ElectionGuard project in particular backed by Microsoft. Other election vendors were using it, and we got to get in on the floor with them and help this process move along.

In that implementation, we did come across a couple of challenges. The first was just a technical one. ElectionGuard at the time was really built for voting systems, right, that you have an offline piece of technology is doing this, and now suddenly we are an online platform that is allowing someone to vote that we need to

do some encryption work in their browser, and that just didn't exist yet, right?

So, with the help of Professor Wallach and some of his students and with Microsoft, we eventually got a project that we were able to encrypt and perform an ElectionGuard encryption on each individual voter's browser. And that was the first like kind of technical challenge.

The second one, though, we really got into is just a regulatory challenge. Most end-to-end verifiable systems are really about returning an aggregate count, right? So we originally thought, kind of naively, if we just utilize this end-to-end verifiability, then we can just replace that. That'll be our entire layer of encryption in this whole thing, right?

But because they're usually striving to preserve voter privacy, one of the common limitations there is that you can't just decrypt any old individual ballot. You just get the total. It'll say this candidate won 400 votes, and that's it. And that's got a bunch of neat math that Professor Wallach talked about.

But the problem is that, today, and for the foreseeable future, states demand that any ballot returned electronically or otherwise must be duplicated onto a ballot, a paper ballot that can be run through the voting system. And so it was that we couldn't use just end-to-end verifiability. Instead, we had to take two different

mechanisms, what I would call more traditional encryption with, you know, RSA and then also apply ElectionGuard as a layer on top of it. This allowed us to do really a check of what I would consider more traditional RSA or more traditional encryption.

That's because, at the end of the day, one of the main things you worry about with software independence is, especially in an online system like ours, is what happens if a hacker gets into the one central location that has all this stuff and just starts changing things, right? If they have the ability to get in there, that's a concern.

And so we utilized ElectionGuard as a separate layer of encryption that really has an offline component and has a voter verifiable piece that allows us to double check and confirm all of those things. So even though I can print and decrypt an individual ballot for purposes of meeting this regulatory burden, I can still run an aggregate. I can run all those through a scanner, find the total counts in that scanner, and then compare that to an ElectionGuard tally and know that it was unchanged, that the totals at least match up.

So this is all to say that there still exist security challenges with online electronic return. I'm not claiming otherwise. Everyone here knows. So what we're trying to do is just say that better is

better, right? And we don't want to be perfect because that just means we're going to use a worse thing in the meantime.

Now, through all this, we did get some feedback from different groups. The first was really our -- I said election vendors. Actually, this is a typo. Election officials generally support it. We've been used in three states in this past election, and there's some kind of mixed enthusiasm, right? In one state, they literally, without any prompting from us, did a whole -- the key generation ceremony, one of the first steps that the administrators take that's offline, they dressed up in capes, and they did this whole thing themselves, right? They were very, very excited about it.

And another one, they take the approach of, we want something that's better. I like what you're doing, you're claiming these things, right? They may not understand it, right, which is a common thing that we're probably going to hear about and we already saw in some of what NIST was presenting earlier, but they still like that we're doing something about it, right?

The second thing is -- we're going to hear a bit in just a minute about what voters think more, but our voters also show a bit of an additional engagement interest because one of the things we get to do with this because we're online, we give them this code back that says, you know, here's your code. You go to this public bulletin board to check it.

But that also serves a second purpose, right? Beyond just checking or auditing the election, you can now use that code to track whether or not your ballot was counted. And for an absentee ballot, this is important because you have a whole process. I sent it back. I want to check it in the mail. You have states across the country that are doing some form of ballot tracking. Did it get to the election office? Was it approved, right, or rejected? Is there some kind of curing process that needs to happen? So they have extra incentive to visit this page and to engage with the system a little bit, which is one of the things we found.

So, you know, all this is to say, especially after COVID, we saw a pretty significant rise in especially people in the disability community wanting to be able to do this. It's become in vogue enough that people have heard that other states are doing it, and they're pressuring their states to do it now. So, again, we're taking the approach this -- we're going to do it the best way we can, and as soon as a better way comes out, we're going to do that, too.

So this is all to say, again, we're not a voting system, but end-to-end verifiability is still really important to this use case and should be important to the other use cases. But I want to point out, for us, this is primarily an accessibility challenge, right? It's not necessarily about trust. It's about accessibility and supporting that

case that otherwise is either not going to be supported or is going to be supported less than securely.

And so that's it for me.

CHAIRMAN HOVLAND:

Thank you, Steven. I think that's several important points, and I'm sure there are going to be questions in a little while. But let's welcome up our third presenter here for this panel, Whitney Quesenberry. Thank you, Whitney, for being here, another distinguished alum of the TGDC and currently the executive director of the Center for Civic Design. Welcome and thank you.

MS. QUESENBERRY:

So it's fun to be on this side of the table at a TGDC meeting.

For those who don't know about the Center for Civic Design, we work with both election officials and technology and advocates across the U.S. to improve the voter experience. We do a lot of work with technology, but our focus is always on how it works in a real election with real voters and real poll workers.

I was on the TGDC. We've been doing research for NIST from 2015 to -- this last year was our last year. A lot of those names were ours. And we were involved with ElectionGuard from the 2020 Aspen project through College Park.

But I first got excited about end-to-end verifiability in 2006-ish when Ron Rivest introduced it at the TGDC. And I just

thought, this is how we're going to be able to do electronic voting, right? Because that's the point of it. So anything that sort of says, oh, no, it's going to be this halfway thing, and we're not going to really get there is not really the promise that we all heard and hoped would happen.

As we've worked with ElectionGuard, we have done a lot of testing to try to figure out how to explain all of this stuff in words that last very few seconds and that mere mortals can understand. And this really interesting thing happened, which is that the more we tried to explain it and how it works in elections, the worse it got. We tried explaining it to general technologists, we tried explaining it to voters, we tried to explain it to election officials, and the more words we used, the worse it was.

And I credit R.C. with what I'm going to say next, but we decided that the analogy is not the airplane or the car. The analogy is your catalytic converter. How many people have one in their car? Do you know what it does? Can you explain what it does besides add to the cost of the car, right? It's intel inside, right, that what we should be doing in introducing new technology is as little as possible to the voter experience, right? Don't make the voter do anything, or at least start from those familiar core steps of someone who just wants to show up and vote can just show up and vote. Make it part of the system, and it's only visible when you have a

moment when you have a choice where you can do something else or just go on.

That was really the core idea about how we were going to introduce ElectionGuard into real elections. I did not do the Franklin County one, so I picked up at version 2, and we learned a lot from that approach.

The first is that it is not enough to say the technology works. Lots of technologies work. Lots of technologies do lots of interesting things. They have to work in a real-world real election with real voters that include the full range of voter experience and capabilities.

Voters actually do want to be able to cast their ballot successfully, and anything that makes them feel like they're too dumb to do it right is a bad idea, but that you can use familiar, minimal design to build voter confidence towards being able to add new things.

We talk about change in elections every time a new technology comes along or a new idea comes along as though elections have never changed, right? Elections change all the time. Election officials produced a miracle in 2020, right, when all kinds of new things happened, and we ran a fantastic election, right? We can do this. We can teach people how to do things. It's not easy, but we can do it.

The other is that -- we call it bite, snacks, and meals where you progressively describe something. Maybe all you need to know is we've added something new to the election system this year to make sure the elections run better. Maybe that's all you want to know. Maybe you want to go to the GitHub site and look at the source code, right? And somewhere in between there is where most of us lived, but everything else comes after the ability to just vote, that that's where you start.

A little bit of the research timeline, we started in 2019, and for a couple years, we ran lots of usability tests trying to work on the language for the key ceremonies and how you explain to guardians what they're doing and how do you explain to election officials how to train the guardians? And at the very last, before we went to Idaho, we did what we called mental model testing where we tried to understand what people thought these words we were about to use meant. We tested icons, we tested short explanations, we tested long explanations. It was kind of a disaster. I mean, none of it got to the point where we thought, yeah, we're going to go into this with confidence.

In Idaho, which is 2022, it was a general election. It was run in one district, in one polling place. We did the messaging research to develop the vocabulary, supported the poll worker training, wrote the training, so we sort of had to actually grapple with saying not

just what we have to do training, but what actual words are we going to say? And we did it again in College Park two years ago for a municipal election that had three days of early voting. It included full support for the ballot marking system. And in both of them, we did voter interviews on election day, so we talked to almost everybody who wanted to talk to us. We came out in force, and we ran a post-election survey asking more questions, and that's where this is boiled down from.

Let me just give you a picture of what ElectionGuard looked like in those elections in real life. There were a lot of partners on this project. One of theories was that if it's supposed to be software independent, all these groups should be able to work together around that core code. And Hart, which is one of the voting system vendors, agreed to be the guinea pig. Ballots were marked by hand, or in the case of College Park, also on their ballot marking system.

The reason why Hart was able to do this fairly easily is sort of an accident of fate, which is that their scanner includes a screen, and it includes a second USB port so you can insert the election definition in one port and the ElectionGuard code in the other, and that sort of made the hardware possible. Our first place was, in fact, a Hart district. So if you look -- I mean, it's a very

familiar-looking voting system. People walked up and they put their ballot in, whatever kind of ballot it was. There's a USB.

There was this moment -- they'd actually done something rather nice with the timing, which is that as the ballot went into the scanner, there was a big pause, and it was longer than anybody would want it to be, but it was just long enough -- it didn't lose their attention, but rather than -- and what happened during that pause was the ElectionGuard read the cast vote record and did the encryption, and then the voter was shown a review screen, the same review screen they would see on the ballot marking system, but on the screen itself at the scanner. And this is an important thing we'll talk about in a second. And as the screen was coming up, the little confirmation code ticket would start printing.

There were a couple of really interesting things that meant. One was that a poll worker, without standing anywhere near that voter, could tell that the code had started, that the scan had been successful. They could tell because they heard the little bloop, bloop that the ballot had been cast, they could hear if it hadn't been cast so that the system -- all the cues the system has for general poll working purposes also worked in our favor with ElectionGuard.

The Benaloh challenge was done -- we called it ballot check -- had to be initiated at the scanner by ejecting the ballot instead of casting it, and then you could get a new ballot to count when you

completed it post-election at the public website. Public website was also built by Enhanced for voters to check their confirmation code, and there was an independent verifier built by MITRE, so lots of people around this thing, but that was the thing. But what voters saw was a ballot and a scanner basically.

Okay. So Franklin County, Idaho, we had really one big research question for this, which was, would we destroy the election? Would we have to stop this in the middle of the day because it wasn't working? Could we get through a day with people actually doing this? And it was a precinct of about 250 voters. Voters were offered the choice to vote the old way or the new way. The old way happened to be central count. They put their ballot in a red box, so they'd never seen a scanner.

And this was actually one of our happy miscalculations. We hadn't thought about the fact that that scanner itself, being able to see your ballot go in and being able to see the review screen come up that wasn't the review screen of what you'd marked on the screen, but a review screen of how the scanner was reading your ballot, sort of gave you this sort of three levels of audit at once, right? You could review the screen, you could see that your ballot had gone in, and this ElectionGuard thing was happening.

We did exit interviews with 65 of the 111 -- it was actually slightly more people because we had some couples -- plus 44

people who had decided not to do ElectionGuard, plus someone from the other district who said, how come we can't do it? So there was quite a mix of sort of old school, like people would say, I'm old school, I want to do it the old way, and people like, yeah, it's something new, I want to try it.

Most of them saw some benefit in ElectionGuard. It wasn't necessarily the cryptography, and that's where the scanner being new came in. Almost everybody said they would check their code. Almost no one actually did. Almost no one actually went to the survey, partly because I think we talked to everyone, and they'd already had their say, right? So we had gotten all of that data. But they said all kinds of really interesting things, like, well, you can test the process to validate the election for non-cheating.

This is a small, rural, red district, and one of our voters, my favorite quote said, well, you know, I do think there's stuff going on in the election. I've been following that pillow guy, and I think he's on to something. But you know what, you guys are the first one doing something about it, not just talking about it. So there was an interest in having a solution, and then we could talk about whether this is a right solution, but there was a lot of interest in that.

We asked because the clerk herself who agreed to do this was on the ballot, it's a pretty risky moment, we said, was she right to do this? Or, you know, is it good to do this thing here? And they

said, well, why shouldn't we get to test the latest and greatest thing just because we're a small, rural county? You know, other counties have problems, and we don't want that here. I mean, they had said all the kinds of things that you hear in the MIT study about distance, and I think that's actually pretty cool.

The other thing that was really interesting was that we were allowed in the polling place to observe, and we had someone positioned where she could see the screen, but she was halfway across the room, so she had no idea what they were reading or not. And we watched people scroll through and scroll up and down. And of those, 111 voters, five of them, that's 4.5 percent for you mathematically inclined, found a problem on their ballot. Two had failed to turn it over and vote the back of the ballot. One person had cast a write-in and wanted to make sure the way it was being reported to him was correct. One person found a mistake. One person found something they'd skipped. So given an opportunity to verify their ballot, people were, in fact, verifying their ballot pretty enthusiastically.

The other thing that was really interesting that happened there was we had given the poll workers a script, right? We trained them. These poll workers were picked because they were enthusiastic about the idea so we weren't facing any resistance. I'll show you in a minute, we had these incredibly cute little handouts.

And, at the beginning of the day, they sort of read what I thought was a very few number of words, but, my God, when you have to say it over again, it was a lot of words. And, as the day went on, they would say, well, what if we said it this way? And we said yes. And we would talk it through with them and let them keep experimenting.

The woman who was closest to the scanner and the sort of lead ElectionGuard person, at the beginning, she would walk them over, and she'd stand with them and make sure it all worked, and then she would walk them over and stand to the side so she was actually staring at their screen. And by the end of the day, she's like, the whole thing had devolved to, hey, we're trying something new. Would you like to try it? So they, in the course of, you know, one election day, had gone from, ooh, this is new and scary, to, hey, this is okay. And then if someone asked them, they could talk about it.

We had one other metric for this, which is because we were giving out these little things, and they were getting a little ticket to take home, as they left the gymnasium, there was a giant trash can, a big, giant trash can. And our question was, how many of these handout materials ended up in that trash can at the end of the day? And the answer was none. Even if they shoved it in their back pocket and never looked at it again, they didn't say, I don't need

this, I'm never going to use it, this is garbage, why are you handing me this stuff? They took it with them and did or didn't go check their ballot.

So this is the report. It's there. I didn't do a QR code, sorry, but there's a long, complicated URL, and it's got reports from all the other partners as well.

Roll forward a year to College Park, Maryland, where they do independent municipal elections, and they were running their own elections, three days of voting in three different locations. We did an exit interview there with 307 voters. That was over a third of the voters and 20 percent of the ones on election day, which is the biggest day.

And, this time, the election officials took much less of a hands-off approach. Janeen Miller, who recently retired as an amazing city clerk, and her board, I'd say, well, I think we should do the poll worker training like this, and they'd go, we're going to take this away and make it our own. And it was great because they weren't going to let us shove anything into their election that they hadn't been through and gone over and made work. And so we worked through all of the steps until they understood it, and they could train their poll workers to do it, and they walked into their feeling confident, and so they could talk to their electeds about it because somebody had to approve this thing.

So generally positive attitudes. We heard things like -- you know, we would ask about the little confirmation code. They'd say, well, it makes me feel like my vote counted. One person actually came up with what I think is one of the languages we should use, which is it verifies twice, once at the screen and once with the code, right? So it's sort of a simultaneous audit.

And a lot of people said, I believe in machines. This is Maryland, where you have a choice of a ballot-marking device or a hand-marked ballot, and they wondered if it was necessary.

But again, my favorite couple coming out, she was a kindergarten teacher and he was a cryptography student at University of Maryland, and she said -- you know, they answered my questions. And she said, I just have a question, and I answered it for her, and she said, okay, that makes sense, but is there a way I can learn more? And I said, yep, we actually have a little Q&A on the website. We had written that for both places and gave her the URL. She looks it up on her phone. She said, this is about the right level of information for me. And he turns to me and says, that's all very nice, but is there anything real out there? And I said, well, there's a GitHub site. And he went, Yes, GitHub.

[Laughter]

MS. QUESENBERRY:

And so there's this thing about being able to give people the short, medium, you know, long, and super long banquet of the information and not starting them at the GitHub site and everything you need to know about in cryptography.

So that was how those elections went. Sorry, this thing I need to read because it's got some stats on it, so I'm just making sure I have them handy. I get stats wrong.

So the voter materials and the handouts were all about balancing accuracy with simplicity. Would Josh Benaloh approve it, and would voters understand it? And so we made what I think may be the best thing I've ever designed in my career, which is these super cute, tiny handouts made by printing one side of paper and folding it twice. So this is how big they were. They literally -- we cut out a corner. They had a pocket to put your confirmation code in.

They started with a one-sentence explanation of how to vote. And the sentence about ElectionGuard was "With ElectionGuard, you know your vote counted and have independent verification that the election results are correct." That was the result of that messaging testing that we did just before Idaho. And then "Here's how you vote with ElectionGuard. You mark your ballot as usual. You review your votes at the scanner screen. You cast your ballot. You take your confirmation code with you so you can confirm at

home that your vote counted." That was it. And there was a brief Q&A on the back which was different between the two places. We had to cut the words down a little bit for College Park because they do two languages, so we had to get it down to half the size of half a piece of paper.

And I think that the cuteness factor about this was an important part of acceptance, right? You know, in Idaho, which is what this picture is, we actually put their "I voted" sticker on the front of this thing. We didn't because it was going to have to cover up the Spanish. But being able to think about something that doesn't feel daunting, where the whole presentation is as simple as we can make it.

The Benaloh challenge was, from the beginning, a challenge. Voters had to decide to run a ballot check. We actually pre-asked some people in the community in both times to do it to make sure that we had some. But the most difficult part about this was not the extra work. The most difficult part about this is that in the configuration of this version of ElectionGuard, it added risks that the voters would junk-mark a ballot and accidentally cast it and that you would end up casting a ballot that wasn't the ballot you actually wanted to mark.

Also, it's a lot to take in what the Benaloh challenge is or what the ballot check is. And we did it one way in College Park.

We did it differently in Idaho. In College Park, we had these laminated handouts that I'm not going to read, but you can sort of see there, which was how to do it so that anybody could pick that up, and you didn't have to know whether they were or weren't doing it. So before they initiated the challenge, no one could positively know that they were going to do one.

I think that the Benaloh challenge is something that you will see more uptake of as people start to learn what it is and they move on to the next thing. It's like you learn how to do the basics first, and then you move on.

A couple of conclusions. The first is that the degree to which we think we're going to develop new technologies without having election officials deeply involved -- and I know that STAR-Vote had Dana DeBeauvoir and her team, but there's a difference between sort of thinking about it and thinking about it when you're actually going to run an election in a couple of months. Each of the clerks said to us at some point, why did I ever say I would do this? But we're going to go on, right?

Because there's this moment because the election is ultimately their responsibility, and we are ultimately outsiders to that responsibility. We're supporting technologies. They have the final decisions and the official voices, and I think that we are too often willing to run roughshod over that and not listen to their instinct.

They might be wrong, but they might be right at the core of it. And the question that you have to figure out if you're the innovator is how to incorporate that rightness with whatever you want to do and make those all work together. And I think early collaborations with more other experts wouldn't hurt either from accessibility to design to voting system vendors.

Building these new mental models are important, and framing them is also important. I love this quote. This is from a 2010 article about the integrity of the election at Takoma Park, where they wrote, "One of the most important lessons learned is the value of close collaboration and clear communication between election officials and the election system providers, whether they be researchers or vendors." I would like to point out that this paper has 12 authors. Takoma Park is a very, very small place. They have one, two people in the clerk's office, some tiny number of people. It would fit in half of this room. They were overwhelmed by this.

And so one of the things I really applaud the Microsoft incarnation of ElectionGuard for was bringing those collaborations from the very beginning. Those meetings were long and they were hard, but they were absolutely worth it.

What do I think is next? I have always thought that the way towards new technology is through pilots, and that you have to

keep trying it out with different election policies, with different voting system vendors, with different ballots, that you have to both work with and accept input from election administrators, that you need open and ongoing support and collaboration across disciplines and people who represent a variety of voters, that you need to focus much earlier.

I can't believe that at the TGDC I'm still saying this, and it's 2025, and we started talking about this in 2002, and that we're still having to say that you can't layer voter experience accessibility on afterwards. You've got to build it in, and that you need to be sharing those learnings so that everybody's understanding what we're putting together as you build it.

So thank you. And I did it in almost my 10 minutes.

CHAIRMAN HOVLAND:

Thank you, Whitney, for that.

And now, we'll open it up for questions for any of the panelists if folks have questions about those. I will throw that out there.

MR. SKOGLUND:

Kevin Skoglund representing IEEE. I'll start with Whitney. I have a question for you.

One of my concerns about E2EV all along has been whether or not the promise to know that your vote was included was

sufficient to voters' confidence or whether they would want to know that it was actually, you know, included and accurately recorded. As an example, I can imagine my mother and my father. You say, okay, you go this website, you can find out that it's in the tally. They'll say, okay, great, it's in the tally. But how do I know that it's right?

MS. QUESENBERRY:

So I also worry about this question because I think we don't ever want to be able to say you can prove how you voted for so many reasons. I don't think I need to go into them. I do think that the events of the last eight years are on the side of I know my vote was counted, and that helps because there was so much discussion about that.

I think that my view of it is skewed a little bit by the ElectionGuard Microsoft iteration technology setup with Hart, which is that they got to see something most people don't get to see, which is how the scanner read my ballot because that same problem is still true on a conventional scanner setup.

So I think the "I marked it, I reviewed what I'm casting, I reviewed what was cast, and I know my ballot was in the mix," might be enough of a chain of control if we can figure out how to explain it sort of really easily.

MR. SKOGLUND:

I guess I'm asking specifically, did users tell you in any of their reporting or anything like that that they had any concerns about that? Did your research pick up on any --

MS. QUESENBERRY:

Crickets.

MR. SKOGLUND:

Okay.

COMMISSIONER PALMER:

Dan, could you talk about the CAC technology? That's the card reader for a military or sort of overseas worker with the DOD. Is that for the confirmation-of-identity part of it, or how is that working with the process that you're --

MR. WALLACH:

Okay. So CAC stands for common access card. Other parts of the government call it a PIV. I don't know what PIV stands for, but it's exactly the same thing, and it's a standard since the mid-1990s for how a credit card-shaped device with little pins on it can talk to your computer.

Inside, it offers digital signatures. It can sign a message in a way that anybody else can say, oh, this message was signed by Dan Wallach, and that was provable because of the DOD certificate authority hierarchy, which is a complicated thing that I won't get into right now. But the idea is that when I send you an email, it's signed

by my card, and so when you open my email, your Outlook verifies this complicated cryptographic chain and says, yep, this was signed by Dan Wallach.

Now, transplant that to the voting world. We can use this in two ways. We can use it both to help make sure we get the correct ballot to the correct voter because now I have a very strong notion of your identity, so we can connect an identity to a blank ballot, thus avoiding a significant challenge that we would otherwise have to make sure that every voter got the correct ballot style because no two voters are from the same original jurisdiction. They're from all over the place when they're on the ship or wherever.

We also use it at the end to cryptographically sign the end-to-end encrypted ciphertext. So we produce an encrypted ballot, but then the machine can stamp it with your CAC card, and that's something that makes it more resilient to tampering in transit.

So the CAC infrastructure helps us on the way in knowing who the voter is, and on the way out, making sure that this is the ciphertext of that voter, all without revealing how they voted, so we still protect voter privacy.

MR. WLASCHIN:

Chris Wlaschin from ES&S. I want to caveat my comments with the fact I've been a cybersecurity professional for 20-plus years, a voting technologist for seven years. I am a fan of end-to-

end verification. What I think is missing, what I think you've scratched the surface on, is what I would call the voice of the customer. I know that there are small vocal groups of voters who are asking for technology like this, the support from the election officials that we've talked to, not so much. And let me give you a couple of examples of their voices.

Chris, I can see how this works in a precinct polling place with a precinct-level scanner. How do you make it work for a vote-by-mail state who uses nothing but centralized scanners? How would you notify a voter that their vote had made it through the scanning process and was counted as cast?

Now there are services out there -- BallotTrax is one of them -- that alerts the voter at every step of receipts, alerts them if there's a need to cure, that it's been tabulated. But how do you create that extra step to say your vote was counted as cast when that vote has been anonymous since the envelope was opened? We've been working on this at ES&S. We haven't been able to solve that just yet. We do have a module that we can put in a precinct scanner that will print the receipt and encrypt the voters' intent.

But another question I get is, Chris, those tabulators, they're encrypted already, right? Yes. So you're wrapping those results in another level of encryption. How can I explain that? So I loved your example of treating it like a catalytic converter and just give

them the bare minimum, figure out how to do that in an era of transparency.

And then, finally, Chris, machine tallies are unofficial, right? Yes. They are unofficial until the election official does their job to certify the election. So in that process, from the times polls close until the election is certified can be days or weeks, and I get this question, you're asking me to post these encrypted results on a website? You want me to do that, or do you want the state to do that?

These are just some of the concerns that have been voiced to us as we move towards E2EV in our technology solutions. So I'd just ask any of you to try and comment on that, please.

MS. QUESENBERRY:

So when I say we need to do more trials, grow it slowly, this is what I'm talking about, right? If you start by saying we're going to do Los Angeles County with 1,500 vote centers, they did launch their thing, but it took them 10 years, right? And they were working for one jurisdiction with one set of laws. I think you build those pieces up.

To go back to some -- sorry, one thing I forgot to talk about was that there's another group that's doing work on the ElectionGuard-based code technologies, and they've been doing some really great testing. And one of the things they just tested,

and I have permission to share this, is an AB test of the value prop for the Benaloh check, which is, is it I can check that my ballot was encrypted correctly, or I can help audit the election? And "audit the election" won by about six points, that people were willing to be enticed into the common good more than they really worried that their ballot wasn't counted because, in general, we kind of hope that it was, and some people are going to be more cynical and less cynical and more willing to take steps.

I think it's really hard to take something as abstract as that and try to think about what that looks like on the floor of an election or, you know, in the real world of an election, and that those are all great questions to ask. Those are questions that should be asked because they're about have you thought about the particular problems of elections that people don't think about? And I think that's why the whole idea of being able to pilot technology.

In Nevada, the way it worked was that because there were paper ballots, they hand counted them at the end of it, so because the scanner wasn't certified in the state, ElectionGuard certainly wasn't certified in the state, but in that case, the hand count of those 111 ballots was the official record, so the state worked with Microsoft to figure out how we could actually do this legally. And in doing so, you begin to think about all the different problems and all the different levels of challenge. But the challenge of a vote center

is simply a computational challenge. It's complex, but not hard. It's just big.

MR. WALLACH:

So I'll just add one thing to the end. You were talking about, are election officials going to publish this stuff? What about all the adjustments that they make during the canvass period? A different perspective you might take on end-to-end verifiability is that it's all about transparency. It allows the public to accumulate the votes and verify the total, but it also means that all of the adjustments the election officials make, every ballot adjudication also is part of this. So you might look at that as transparency. You might look at that as airing dirty laundry.

In an era where any correction that an election official makes could be amplified as a form of misinformation, you have to say that transparency could be the antidote to misinformation, and the end-to-end techniques can create that transparency.

MR. MUSICK:

Real quick, I just wanted to address kind of the three problems you brought up. Hopefully, I remember them all. The first was kind of, you know, a voter votes, and they need to track their system like they would in BallotTrax, obviously. In our case at least -- I can only speak to our use case -- that's fairly simple because we have a confirmation code and we know the process that that

confirmation code has gone through between approval, curing, eventual decryption, and then the final election record once it's actually been decrypted, like the whole tally has been decrypted. So we at least can convey that information very similar to the way BallotTrax would.

MS. QUESENBERRY:

BallotTrax --

MR. MUSICK:

They're just doing --

MS. QUESENBERRY:

-- they'll tell you that it was received. It can't tell you that it was --

MR. MUSICK:

Yeah.

MS. QUESENBERRY:

-- counted.

MR. MUSICK:

They're just doing through the USPS, but we're --

MS. QUESENBERRY:

BallotTrax can tell you it was received, but not that it was counted.

MR. MUSICK:

Right. So similar, the second thing that you mentioned was kind of vote by mail. This is just something I happen to know. I do know that the latest version of the ElectionGuard specification, 2.1 I believe it is, does include a mechanism by which you can preprint pieces, short codes of what will become -- based on what you vote for, determine your whole final code, and so that it can actually be used in a vote-by-mail scenario, so that there -- I don't believe any implementation has done that yet, but it exists in the specification.

And then the third scenario, I don't remember the question, I'm sorry.

MALE SPEAKER:

Unofficial results --

MS. QUESENBERRY:

Vote centers. Vote centers --

MALE SPEAKER:

-- why --

MR. MUSICK:

Oh yeah, the certification and such. And the truth is that kind of, as you mentioned, right, you do that as you go along. But also this really starts as an offline process where you do the decryption offline with the election administrators, and at that point they can do that whenever, and then their process makes sense to them, probably before certification so they can use this to help

decide whether or not to certify. And then, ultimately, you probably don't post until you've actually certified the election. So from our perspective, we get one big record once they agree to release it to us, which is up to the election officials.

MS. QUESENBERRY:

It's not that different than the ranked choice voting challenge. I loved watching Shenna Bellows, who's the Secretary of State in Maine, because they did a full state recount of one of the elections. And, you know, so they talk about it and they do the explanation. They said, okay, is everybody here? Is everybody watching? Everybody ready? Because we're going to do it. Bunk.

MR. WLASCHIN:

Great responses, all. Dan, your comments about transparency reminded me of the one request we got that resounded with me the most, and that was an election official said, Chris, you would solve 90 percent of my problems if you could make that ballot box transparent so the voter could see their ballot dropping into the box. It could be as simple as that. But thank you for wonderful presentations today.

COMMISSIONER PALMER:

Chris, visiting some foreign countries in their elections, I have to say the transparent box really is sort of an attractive

feature. It's really fun, and it's very obviously transparent. It's a thought to think about.

CHAIRMAN HOVLAND:

VVSG 3.0.

[Laughter]

MR. SCHOELLER:

Shane Schoeller, Board of Advisors. So quick question as an election official, so does the voter and the election official get a paper copy, or, once it gets to the election official, is it all digital? Of the ballot cast. I don't think that's --

MR. MUSICK:

It's going to depend on the implementation.

MR. SCHOELLER:

I'm sorry?

MR. MUSICK:

I said it's going to depend on the implementation. I know that the way some voting systems have done it, they would actually have a single ballot that is printed that would go in the ballot box, just like everything else. What we saw with Hart, actually, that was the system. And then the voter got a separate piece of paper that contained a code.

In our system, right, being an absentee system, it's delivered purely electronically but then duplicated onto a paper ballot from that point.

MR. SCHOELLER:

So you'd have a team that would take that and then transcribe it to a regular ballot is what you're saying?

MR. MUSICK:

Yes, and --

MS. QUESENBERRY:

I mean, the Idaho/College Park model, if we're going to stay on internal combustion engines, is kind of the Prius.

MR. SCHOELLER:

Right. I think from an election official perspective -- and I want to continue to put great caution on this, I understand it for military potentially, people, can I get there? I would never endorse it for every voter, first of all. It just makes no sense. Second of all, transparency is only as good as the knowledge base of those who understand what's -- and I don't mean that -- you have to be transparent. What I've seen in elections is people don't understand the processes that are taking place. Then you actually see social media things that are put out there that actually malign what was taking place --

MS. QUESENBERRY:

Yep.

MR. SCHOELLER:

-- because they put out false information. So we have to endorse transparency, transparency that has great knowledge and understanding. I've said you almost need to have a play by play when you have the cameras there to explain to people what's taking place, or otherwise it can become a bigger problem. So we do have to have transparency. We have to have it so that people understand what's taking place.

MS. QUESENBERRY:

Absolutely. One of the most important documents we wrote -- and we wrote it in Idaho and adjusted it for College Park -- was the Q&A. It had who everybody was, what everybody was doing. It walked through common questions. It did all the things, and it was the talking points. And the idea was that all of us should use that language so we didn't go off on our own paths because the minute you start using different words, that gets confusing.

In Idaho, a paper letter was mailed to every voter in the district that was going to have the option in advance. They had stuff in the newspaper in advance. And lest anybody think that election officials don't know where the flaws are, we were describing the whole thing and the guardians and unlocking the thing at the end, and one of the two guardians was the former clerk,

now quite emeritus, and she turned to the current clerk and said, so listen, Camille, I'm getting on in age. What happens if I drop dead between now and then? It was the fingerprint line. And Camille said, we'll be down to the funeral parlor getting your finger.

[Laughter]

MS. QUESENBERRY:

Right? I mean, and she just listened once, and it was like she was right on it. So we did that. So there was a lot of layers of communication.

In College Park, they actually held a public meeting so that they could walk through it if anybody wanted to come. And then they did a public meeting afterwards so that people had a chance to come in and ask questions and try out the accessible voting machine that they were using for the first time and all the rest of it. And they got it in as many papers as they could. They had students come. So in both cases there was a lot of attention to communication, maybe more than almost anything except the encryption itself.

MS. GOLDEN:

Diane Golden. Can you clarify for me the remote ballot delivery and then electronic ballot return? Is there an E2EV code involved in that --

MR. MUSICK:

Yes.

MS. GOLDEN:

-- also, and is that delivered digitally? I'm assuming same mechanism used to deliver the digital accessible ballot?

MR. MUSICK:

Yes.

MS. GOLDEN:

And then it's marked online using their own IT/AT, and then somehow it's returned digitally, and then they get a confirmation code that lets them do all this backend stuff?

MR. MUSICK:

Yeah, so the short version is that once --they get the traditional online marketing experience that someone would if they were doing a vote-by-mail ballot. They go through all the way through the end where they make their selections, they review them, and then they get to really one extra step, which is a bunch of stuff happens in the background, kind of as Whitney said earlier, transparently. We're doing a couple different encryptions that we're using to verify each other.

And then at that point, once that has been encrypted, that's when we present the code to them, so they receive that on the exact same application they're using where they marked their ballot, so same accessible interface. And then at that point, they --

we also give them a way to copy that so they can save it and a link to the public portal to go check it. And, in that case, we actually have automatically synced it over with just the status of we've received it as soon as we received it, but nothing else has happened yet. They can come back there to check not just whether or not it was finally included, but also the other pieces of that process.

MS. GOLDEN:

Since I screwed this up once, I didn't want to screw it up again. Sorry about that.

[Laughter]

MS. GOLDEN:

Cool, and I'm just going to say kudos for the whole presentation, which is, okay, we realize this isn't perfect, people, but the alternative is these people are disenfranchised. That's the bottom line. And this is not about opening this up for everybody and their brother to do. This is about people who have no other way to vote maybe at all, let alone privately and independently. We're not asking for the moon here. We're just asking for you to give us an inch so we can finally get over this hump.

And I mean, I've said it before, I'll say it again. At some point, you've got to be willing to take a little bit of a security risk to get accessibility to people who have been denied it for 20, 25 years

now. I just hope we're past finally where we've been entrenched in this battle that we can say there are some people we need to make an exception for, please.

MS. QUESENBERRY:

One of the things that makes me say so loudly that the election officials have to be part of this process was a paper we did where we interviewed people who were doing accessible vote-by-mail systems, and we were just interested in the uptake. There were places that had lots of people using it, places that had very few people using it. We were sort of curious what was going on. This was semi-structured interviews, not nearly as rigorous as what the NIST of this did.

But the biggest thing that came out of that paper, for me, was that the barriers were not willingness, were not interest, were not interest on the part of the voters necessarily, but that there were just these technical gaps in getting the data from the voter registration system, from the election management system into the accessible voting system, and that, as the years went on and they learned to do it more, the states and their counties learned how to do this more efficiently and figure out, you know, how to make it possible for a small jurisdiction to manage this in the middle of a running election.

So there's a kind of administrative learning process, and what you want to do is not try to pile everything in on the first step because it will fail then, and then this idea, which might be fabulous, will be gone forever. But if you can figure out what the stages are, and how do you get from here to there, and how do you build the confidence of the people who are in charge of making sure that the right voter gets the right ballot and it gets returned in the right way, I think you can get to the point where you can solve a few problems every cycle and grow it in scope at the same time.

MR. SKOGLUND:

So I have a couple of questions, primarily for Steven and Dan. So the two central promises of E2E verifiability is being able to determine cast as intended and to be able to determine tallied as cast, right? And software dependence really depends on being able to prove that. So my first question is for both of you. How do your systems allow the Benaloh challenge so that you can spoil a ballot, which is kind of critical to proving that first promise of cast as attended?

MR. MUSICK:

I'll speak to ours, and I'll say that the truth is, this is one of the places where we take a little bit of a hit. The second step there, I forget the exact terms, but that it can be tallied and you can prove, that's all solved by ElectionGuard in the election record when we

publish it and they check their public bulletin board. So to the degree that ElectionGuard can prove that, we can prove that as well just by using ElectionGuard.

That first step is a little bit different with the Benaloh challenge for us because of the fact that we are voting with separate devices. In a normal voting system scenario where you're at a polling location, you have many voters using the same device, and all you need is a very small percentage of voters to perform this check on this one device to know that most of your devices are probably safe, right?

In the absentee voting world, particularly in this case, each person really has their own separate device, so even if I can prove that one device is free of malware, that tells me nothing about the 99 percent of people that did not perform this check. So this is the one area where I'm going to say we're going to do it as good as we can. We're using, what I would say, end-to-end verifiable methods, but I can't say we're purely end-to-end verifiable yet because of that.

MR. SKOGLUND:

That's an excellent answer because it's something I didn't even think didn't even think about. I was asking more just, is it possible to sort of get all the way through the process and then spoil the ballot using your system?

MR. WALLACH:

So I would say that's really the essence of the Benaloh challenge. If you look back at his original 2006 paper, his conception was that it would print a ballot behind a screen where you couldn't see it, and then the voter would get one extra question, cast or cancel. And that was a usability nightmare. And the newer versions have -- sorry?

MS. QUESENBERRY:

Actually?

MR. WALLACH:

One of the fun things I learned from usability is they love to talk about early ATMs. The first generation ATMs, you would say, give me $100, it would put the money out, you take the money and leave and leave your card in the machine. And it took them a couple generations to realize that the ATMs -- every ATM today makes you take your card before it gives you the money. The usability people call this an after-completion error because your task is get money.

Anyway, what does that mean in the voting space? We need to make sure that however we're going to instantiate the Benaloh challenge or some other challenge process has to not get in the way of the standard voting process. And ElectionGuard is a toolkit. It doesn't say, this is how you do it. It doesn't specify the

user interface. It just says, here are the APIs to get at what you need.

And beyond that, like if you were going to do it as a ballot-marking device style system, then you'd probably do something like what we came up with for STAR-Vote where the physical motion of the printed paper ballot from the voting machine to the ballot box or to the front desk where you're going to spoil it, that's the Benaloh challenge embodied in physical motion. There are other ways you could do it if you're going to do a hand-marked paper ballot or other styles. The key thing is that there's always a clever way that you can do it without getting too much in the way of the regular process.

MS. QUESENBERRY:

So the College Park election -- I'm just going to say College Park, Idaho, as a way of distinguishing them. The flaw there was that you couldn't actually complete the Benaloh challenge until after the election. But the moment for it happened after you had read the screen, the ballot had been printed, and you said "eject" instead of instead of "cast." So it happened at that moment of casting. So it's essentially the same thing as that.

Tusk data -- I have to read it because it's not my data -- they did eight mock elections with 445 ballots cast, and they had 214 ballot checks performed. Because they're doing an electronic

return system, it happens at about the same time you said, which is up on the screen. And unlike a paper ballot, you don't have to take that ballot away from them and get them to remark a new ballot. They could just say, yes, I've checked it, and I wish to send it on.

Interestingly, they tested with blind and low vision and had 62 percent of the people, the largest number of people do a Benaloh check. Gen Z voters at the other end were at 52 percent. So given a moment when it's a fast moment in the system, people took the opportunity for it. It was a test. It wasn't a real election. Let's, you know, be clear about all that stuff, but nonetheless, those are pretty good numbers.

MR. SKOGLUND:

And the second half of the question, if I could, just about the other key promise of E2EV, which is knowing that your vote was included in the tally. It seems to me that in these remote situations that you cannot verify end-to-end, you can only verify end-to-bulletin board, and that at that point it has to be taken out, and you don't actually know whether those votes were extracted and included in the tally.

MR. WALLACH:

Oh, no, you do. So every voter leaves the polling place or can leave the voting place with a hash of their encrypted vote, so that doesn't --

MS. QUESENBERRY:

A confirmation code.

MR. WALLACH:

Yeah, a confirmation code, sure, we'll call it that. But what it does is it lets you prove that your encrypted vote is on the bulletin board. And then you or anybody or perhaps more likely your newspaper or local civic organization, like, you could imagine the League of Women Voters renting a bunch of servers from Amazon on the evening of the election, and you go to your favorite, trusted civic organization, punch in your confirmation code, they'll tell you yes, it's on the bulletin board, and that bulletin board yielded this total. And so were your ballot not included, then it wouldn't add up.

MR. SKOGLUND:

I appreciate that. I guess what I'm saying is the bulletin board is not the end of the journey, right? There's another last mile there that is you don't actually know that it's included in the tally of the election, just the bulletin board.

MR. MUSICK:

Well, I want to also include one way that I can additionally prove this, just to show a case, how it works in our system is that when we've printed out the ballots to be included in the voting system, right, because I know some of the voting systems using ElectionGuard also keep two records, effectively. They have their

internal record they already had, plus the ElectionGuard record. And that's similar to our scenario where they've printed out a ballot and I have the ElectionGuard record.

And so what I can do is, once I've run all those printed ballots through the scanner, I know every candidate got 400 votes, 300 votes, et cetera. I know the totals. I can compare that to the election record and see the exact same totals. And so long as I know that the totals are identical and that all the codes are included because I checked it, then I can prove that my vote was included in the tally.

MS. QUESENBERRY:

Yeah, in College Park we sat there in the big assembly room, and the guy from Hart read out the totals from the Hart -- actually, he handed the piece of paper to the clerk to read them out, and the guardians unlocked ElectionGuard, and we read out the ElectionGuard totals. And by then we posted it to the bulletin board, or it had been posted to the bulletin board -- you check me if I'm wrong -- and MITRE ran their verifier against it. And so we had three totals reading the same election but not actually reading the same identical package, the physical package because one was on the bulletin board, one was on the USB chip, and one was there.

MR. WALLACH:

So the one piece I think that you might be getting stuck on is that the thing that anybody can do with the public bulletin board is add encrypted numbers to get another encrypted number. Now you say, what's the point in that? So the election officials, this guardian process, they produce the decryption and a proof, and that proof is mathematically convincing that this encrypted total yielded that proper decryption. So that's a proof that's convincing to any observer, and that's what ties it all together and creates the end-to-end.

MS. QUESENBERRY:

And to claim that your independent verification is different, you have to show your proof matching those proof points. I'm going to say that in a very -- that's the limits of my technical understanding. But you can't just say it's wrong, right? The proof process essentially prevents a denial-of-service attack. Is that good enough?

MR. WALLACH:

If we had a whiteboard, I could do some math, but sure, let's go with that.

[Laughter]

MR. WALLACH:

No, the proof process is what's called a zero-knowledge proof. It's a proof that only by -- because I know the secret key, or

in this case, the secret key spread across multiple guardian people so no one person can do the decryption operation, it's a collective operation, it's a proof that they did it correctly.

Anybody observing -- and I want to emphasize, this could be your favorite political party, your favorite civic organization, your favorite newspaper. Anybody can look at the public bulletin board, the decryption proof, and any number of the confirmation codes and agree that these confirmation codes are on that board that was added up correctly and add decrypted correctly. The whole thing is public and verifiable.

MR. SKOGLUND:

I'm 100 percent with you on the bulletin board. I completely have faith in the homomorphic encryption and everything. It's just that last step. It seems like at some point, election officials have to take things off the bulletin board and combine them with the --

MS. QUESENBERRY:

It's the other direction.

MALE SPEAKER:

It's something anybody can do.

MR. WALLACH:

Yeah, anybody can do that operation. The only thing that the election officials can exclusively do is decrypt the total, that's it, that one last step.

MS. QUESENBERRY:

Can I translate? Let me translate this into the language I understood, which is, Josh said, the whole key to this homomorphic encryption thing is that anybody can operate on the contents without opening it, right? So without being able to get to the individual things, you can ask questions like, how many people voted, how many spoiled ballots were there, how many people voted for this thing, but you don't have to actually get into the inside. Only the election official and the guardians could get to the inside. For anybody who's at my level of technology, they're wondering what the heck they're talking about.

MR. MUSICK:

And I'll just add on, obviously, they talked about all the homomorphic encryption and all that. And once you get to that point, anybody in theory can take that point and then go compare it to the certified results or the results on the ENR pages, et cetera, and they should match one to one.

MS. QUESENBERRY:

Yeah, there was big cheering in that room from some people and like, from everybody else, right, because it might not right. And, in fact, in one of the times we ran it, there was a problem. We were able to go, oh, yeah, where is it? Oh, it's here. Because that's because we updated the software, and you haven't updated

your verifier. So they were able to do that fairly quickly and right in front of a group of people.

CHAIRMAN HOVLAND:

We are at time, but I'm going to add one more because I think it will help our conversation after the break. And I know some people want to just wait a little longer to go to break.

[Laughter]

CHAIRMAN HOVLAND:

So E2EV was included in the VVSG 2.0 recommendation from this body and ultimately in the adopted VVSG 2.0. Most of the work that was described here today was after that adoption. Obviously, much of this technology is still emerging, but we know more now than we did in February 2021. I don't know if you have any thoughts that you would want to share about what are some of those critical elements or lessons learned that are relevant to a certification standard or what we would be looking at when you think about the VVSG and what you would need to be able to test and verify to say that an end-to-end system is truly what it's intended to be.

MS. QUESENBERRY:

So I'll do the nontechnical answer, and then I'll turn it over to you guys. It seems to me there are two different problems here. One is certifying the encryption itself, that that belongs, you know,

in the world. And who was it who said, don't ever roll your own encryption, right? Yeah, that that should be a black box to it.

The other piece of it is how do you turn using that encryption into a product? And that's what people like Chris do, right? That's what a manufacturer does, is you turn it into a product. And I think that was the challenge of the piece of ElectionGuard I worked on was that we both had a team of technologists figuring out the encryption and how to make the code work and figuring out how to make it a product at the same time, working with Hart. And it's never going to be a nice, neat, tidy thing. When we think about what you have to test to certify it, those are separate, right? Doe this encryption work, and does it do all the things that a voting system needs to do?

MR. WALLACH:

So we need to think about certification as a layer cake. At the bottom, there are the cryptographic operations. How big are the keys? How long are the ciphertexts? How exactly do we do hashing? How exactly do we do each of the internal technologies? These are the kinds of things that NIST happens to have a lot of experience at. Also, our friends at certain three-letter agencies have a lot of experience with this. And getting all of those parameters just right is a sort of nerdy in-thing that the right nerds need to be in the right room and argue with each other about.

But as you go further up the layers, we're going from cryptographic primitives to how do we design a ballot to how do we operate an election? And we need to work standards at each level of this layer cake.

MS. QUESENBERRY:

And synchronization to some extent.

MR. WALLACH:

Yeah. And they will inform each other. So at the top level of the layer cake we need to be very careful -- I mean, that's where the Benaloh challenge or other things like it go. So we need to make sure that the user experience doesn't compromise the security story, or vice versa.

MR. MUSICK:

Obviously, I don't want to speak too much because we're not a voting system, and I don't want to pretend to speak for the voting systems.

I like his analogy of the layer cake because at the end of the day, a lot of what we call E2EV right now exists in academia and is really beholden to peer-reviewed research because it's complicated, it's math-y, and the average testing facility doesn't have the capability to test that, right? But if you view it as a layer where you can end up with is you can say, if you're rolling your own math, you have to go through this really complicated process to get

it, but if you're using one that maybe we've already pre-certified or something like that, then we can just say, have you implemented it correctly?

MS. QUESENBERRY:

And you have to take seriously all the perspectives, right? The reason why the TGDC has the statutory requirements it has, the reason why multifunction, cross-disciplinary teams are important. One of the crazy challenges we have as a qualitative, practical researcher, as an academic researcher is getting academic researchers to take our work seriously because they have an epistemology that says if it hasn't been through a certain kind of peer review, it doesn't exist. And we say if you haven't put it up against real voters in a real place, it doesn't matter. And bridging those two is hard, but it has to be done.

CHAIRMAN HOVLAND:

Well, thank you all for that.

And with that, we will go to a 15-minute break, 14. We'll see you back here at 3:20 where we will continue the conversation. Thank you.

[Recess 3:06 – 3:23pm]

CHAIRMAN HOVLAND:

I hope everyone had an excellent break. We will now power through to the end of our meeting, but this should be an excellent

portion of the day, look forward to some good conversations. We've blocked out this time, really, for a couple discussion topics, feedback for the agency to think about or consider, some of which will hit on some of what we've talked about today, but with some of that robust E2E conversation there, I kind of want to move that one up, but I think I'll save it as dessert.

[Laughter]

CHAIRMAN HOVLAND:

For those of you that are new to TGDC meeting, this is the flavor of the TGDC. We are going all the way down the rabbit hole. And so, again, a couple things that we had wanted to raise and talk about areas of sort of awareness, but trying to think about how best to have the EAC and our Testing and Certification Program engage on these topics. And so one of those was nonmanufacturer vendors, you know, thinking about the people that participate or have a significant role in a number of states with a number of local jurisdictions, often resellers for the major manufacturers, again, often playing a very key role in the election administration process, but an area that there isn't a lot of visibility, and so something that we've been thinking about how we might look at that within the program manuals or otherwise.

And so just to sort of start this discussion, I wanted to throw out a couple things that we've been kicking around on how the EAC

could potentially get more visibility or have a better understanding of this portion of the election administration space. And so, you know, option A here is doing a study, doing research, as the EAC is designed to do, on the sub-vendor landscape, looking at which vendors are used and what services they provide, how they're contracted and managed around the country or in some subsection.

You know, another option would be within the program manual and the manufacturer registration process, requesting additional information on sub-vendors to have that understanding. And certainly, this is also something, you know, that, again, we could kick down the road and talk about as something that would be included, potentially, whether or not it's the Election Administration Voting Survey, or EAVS, or we've been looking at an off-year vehicle as a way to collect additional information around elections.

So I wanted to just sort of throw this out for open discussion and get feedback if this is an area that's worthwhile to pursue and if any of these thoughts stand out as being a particularly fruitful avenue, or if there are other ways to think about this that maybe we're not.

I think really, in my mind, the goal of thinking about this area is, again, recognizing that this is an important part of the election ecosystem. It is often one without a lot of touchpoints, certainly not

at a national level. And as we look at both the functionality of voting systems, but certainly the security voting systems there is an important component and nexus here.

And so I wanted to, again, just open this up for conversation, for thoughts, for recommendations on ways that we could approach this. And if no one has ideas, I'll make them up.

[Laughter]

MR. WLASCHIN:

Chris Wlaschin, representing the manufacturing community. There are several vehicles out there, several groups that have formed and coalesced around election technology, manufacturers, service providers, and stakeholders. Nearly all of the voting system manufacturers, many of the pollbook providers, and the emergence of electronic ballot delivery and other systems that that jurisdictions use are trying to be -- we've invited them to join the Subsector Coordinating Council. You know, we have probably 40 members, 45 members in the Subsector Coordinating Council. The IT-ISAC special interest group has far less than that, but also a number of election technology manufacturers and service providers.

There is something to be said for registered manufacturers being represented in this group being subject to the voluntary voting system requirements that the EAC and this committee help define. As you know, there's a whole other world of technology out

there being used by election jurisdictions, so I think it is worthy of a study to figure out how to involve all of those other service providers. And I'm talking about the small and medium ballot printers that states and local jurisdictions use. They all play an important role. I think it's worthwhile to study how to involve them, to capture their voice, their input, their needs that could be considered by this group.

CHAIRMAN HOVLAND:

Thank you for that, Chris. You know, I think you raise an interesting point there. I think, you know, it is interesting to think about sort of the different categories and different services. You know, I know one of those, of course, and one that is, as we think through the options that I sort of mentioned, you know, of course, for the registered manufacturers, they know who they work with in particular states and maybe who represents them to certain customers. You know, that one would be probably a more natural fit for something in the Testing and Certification Manual.

But that doesn't touch on other areas like you just highlighted with ballot printing and necessarily -- and some of the things, you know, thinking about -- you know, we just did a 2024 sort of lessons-learned hearing in December, and some of those things that popped up, some of those headlines that we saw in the 2024 election, you know, there were pieces of that that were very much

part of that story. And so, you know, that does make me think about some of the wider sort of survey-type instruments as well to get a better picture of that landscape. Thank you.

COMMISSIONER PALMER:

Commissioner Hovland, on the use of the EAVS, what kind of questions do you think might be helpful, and, you know, what could we receive from the localities, just the name of the vendor that they're working with and what sort of services are being provided?

CHAIRMAN HOVLAND:

Well, and just to make sure that we don't get a lot of hate mail --

[Laughter]

CHAIRMAN HOVLAND:

-- I know people are very sensitive to changing EAVS, so, you know, in some ways, I would think that, you know, this might be one of the other vehicles that we were talking about. One thing that's worth knowing, you know, we're very much considering a survey instrument that that runs in opposite years of EAVS. I'm trying to get us to call it ODDS so that we have ODDS and EAVS.

[Laughter]

CHAIRMAN HOVLAND:

I don't know if there's uptake on that, but now that I've said this publicly --

[Laughter]

CHAIRMAN HOVLAND:

-- I hope that it happens.

COMMISSIONER PALMER:

Now you will get hate mail.

CHAIRMAN HOVLAND:

Yes.

[Laughter]

CHAIRMAN HOVLAND:

So to your question, yeah, I mean, I think that, certainly for us, and certainly part of the feedback question here is probably striking, you know, what is that right balance? You know, obviously, we are cognizant of the fact that when we ask jurisdictions to be kind enough to fill out those surveys, you know, we don't want to overly burden them. We're not asking for every contract, you know, that they've ever had. But I also think, you know, this space has certainly evolved, and I think some of the security elements of that.

But then, you know, one of themes that we've heard several times today that intersects with that is communication, and so when I think about, you know, some of what we talked about earlier with

Field Services, when I think about some of the issues that have popped up in the past, sort of having a picture of that landscape, having an understanding of the players involved and where an issue might be, to be able to sort of as quickly and accurately respond to that and try to find a solution, you know, if that's an anomaly issue, if that's some other issue, you know, having that roadmap ahead of time, you know, that's the sort of the business card exchange ahead of the storm that you hear people always reference.

And so being able to know -- you know, have more visibility into some of the ecosystem, again, looking at that diversity across the country, I think just having a sense of that and those commonalities or pinch points is certainly something that could be of value.

We have time allotted for this, but we also don't have to belabor it. And I do know we're in the afternoon, and I know that people really want to get back to end-to-end and our dessert, so I'll do a quick going once, going twice, sold here. All right. Do whatever I want on that one. Thank you.

[Laughter]

CHAIRMAN HOVLAND:

The next thing that we wanted to talk about before we get back to E2E is component certification. Again, I think this is a really

interesting topic. Again, in the Testing and Certification manual that came along with 2.0 was a Component Testing Pilot Program. And really this was meant to examine the feasibility of testing and certifying components as part of existing EAC-certified voting systems. However, it didn't really envision like a standalone component that would be system-agnostic, and the only interaction would be the intake and production of data in the common data format.

We recently received some inquiries from vendors who would like to provide standalone tabulation systems, particularly for ranked choice voting. There's also the possibility of handling these systems through our ESTEP program. And so I was curious about what feedback there might be or thoughts on considering standalone components. Certainly, you know, there are elements of, again, the common data formats of interoperability that lend themselves to that, certainly aware and want to encourage, you know, a healthy election technology ecosystem.

And so I would like to just sort of put that out there for conversation, you know, how we should be thinking about the potential for component certification. And I know some of -- oh, come on down. David, thank you.

MR. WAGNER:

David Wagner. I'm wondering if you might be able to share with us anything more about what the asks or the needs of these vendors might be, what they might need from a standard to support these alternative tabulation systems. For instance, maybe you could say a little more, are they asking for additional requirements in the standards that all the other systems have to support so that it's possible to have an alternative tabulation system, or is it more of the form that they want a path to certification for their product, but they don't need the rest of the ecosystem to change?

CHAIRMAN HOVLAND:

Yeah, I think that it's more the latter. And anyone from the Testing and Cert team or otherwise, when I wander off out of my depth, feel free to come up and chime in if you want. But, you know, I think some of those instances where we've seen it or could envision it, you know, as it stands, certification under the VVSG is for a total voting system, and that is a fairly, you know, broad endeavor.

And so I think you see folks -- the example I used earlier with ranked choice voting, obviously, there are people out there that specialize in that. That certainly could be software that's included in an existing system and then brought in for certification, and that could be a piece within a broader certified system. But I think what some folks are looking for is if this has been tested, if this has been

certified in a standalone way, then they're able to potentially -- market might not be the wrong word, but are able to reference that it has at least passed that level of review, whether that's for inclusion in an EAC-certified system somewhere, whether that is going to be used sort of separately by a jurisdiction.

You know, I could imagine this particularly -- I also see a lot of potential applicability in the assistive technology realm. Maybe I want to make a BMD, but I'm not interested in being in the scanner business, and so, you know, thinking about the potential for entities to not have to take on the whole of the voting system as it's currently envisioned.

MS. GOLDEN:

Diane Golden. I promised myself I wasn't going to comment on this, but since you opened the door -- sorry about that.

[Laughter]

CHAIRMAN HOVLAND:

Why would you promise that?

MS. GOLDEN:

The challenge with component -- and personally, I don't have any strong feelings for or against or how or anything else related to component testing and certification. The challenge with anything voter-facing and accessibility is, with a paper ballot, you have to do the entire process of marking, verifying, and casting in the same

physical area because you have a paper ballot moving, and you can't have, you know, a precinct counter in a different room or down the hall because that paper ballot's got to move that whole way, and all of a sudden you've got another access problem, barrier.

So separating tabulation, as long as tabulation casting isn't connected, you know, therein lies the problem. If it's a precinct counter and that's the ballot box, then again, just because of the access challenges of paper, it pretty much -- if you're going to satisfy 2.0, it's going to all have to be there together. And you can't un-test it together because it's one fluid process. So it does have to have a scanner because you have to be able to verify. You know, so it just introduces this again.

In my utopia where everything's digital, this would not be a problem because you can move digital things all sorts of ways, but that physical paper ballot really introduces a physical limitation to components, too, until you get to that point of casting and then the voter's done, and yeah, you can do your tabulation. That's a whole different issue.

So this came up in discussions with the testing people because of the RFI request and the whole idea of different pieces of equipment doing different things. And when it comes to the voter-facing process of marking, verifying, and casting and

accessibility, you're just stuck with everything being kind of together.

CHAIRMAN HOVLAND:

I thought you promised you weren't going to comment. No --

[Laughter]

MS. GOLDEN:

Sorry.

CHAIRMAN HOVLAND:

-- I'm joking. I really appreciate those flags. That is excellent feedback and why we asked.

MR. SKOGLUND:

Kevin Skoglund representing IEEE, thank you. The first thing I would say is that I think we need to -- component testing is too broad of a term. I think we need to break that down because the difference between someone needing a rank choice tabulation system is very different from the idea of I want to have two different vendors in my precinct, or I want an EMS by one company and a tabulator by another company, right, to sort of mix and match. I don't think that's very viable. I think there's so much that's programmed from the EMS and then shared to all those devices that I think is proprietary. It's not interoperable. And I think it's going to be hard to have components like that. So you can just buy a new central count scanner, and maybe it's not from the same

person your previous central count scanner was from. I don't see that happening.

But the idea, like the ranked choice voting, I think New York State requires systems to be certified, but there was no certified system that could do the ranked choice calculations. I think that was the gist of the problem they ran into. And I think in that case, there does need to be some mechanism. But at the same time, if they're not having voter-facing devices, maybe there's a subset of requirements or something like that that they have to fulfill instead.

CHAIRMAN HOVLAND:

Yes? You're in my blind spot because of Don. Sorry.

MR. WAGNER:

David Wagner here. I don't know if this will be helpful, but I'll share some thoughts. I imagine the EAC might be thinking about how to prioritize the limited resources on all these different possible initiatives and so some possible thoughts in case it helps.

When I'm thinking about the promise of component certification, the hope would be, the dream would be providing more options to election officials. And so I think about kind of when you consider potential initiatives in this area, I'm thinking about what's going to be the value to election officials, and, like, what's the technical feasibility? And so that might depend on what kind of component we're looking at.

So if I think about alternative tabulation systems for ranked choice voting, that was one example that was mentioned, I think, in terms of value to election officials, that might like a narrower audience. Maybe there's a small audience where it would really like that, and then many election officials where that's just not relevant. So I don't know how to assess what the value is, but I imagine that's more limited value to election officials.

And then from a technical feasibility standpoint, my suspicion, without having studied this, is that that's probably pretty feasible, that just the aggregation functionality seems like something that's pretty separable, ought to be testable, and so I would imagine might be suitable that you could develop some standards that would enable a system like that to be tested and certified. My guess would be that it would need to be -- if you were going to test an alternative tabulator, it would need to be tested in conjunction with some other voting system and maybe certified for use with another voting system rather than general certification, you can use this with any voting system, so that in terms of technical feasibility, that seems more doable.

And then for something like alternative devices for accessibility, what I just imagine is the value of that could be substantially greater, but the technical feasibility sounds a lot more challenging, as Diane is pointing out. And so I just don't know

whether there's, like, you know, market appetite and companies that would take advantage of that and whether that would be a valuable initiative.

So I don't know what the answers are, but those are the factors that are going through my head as I'm thinking about is this a good priority for EAC to spend its time on?

MR. WLASCHIN:

Chris Wlaschin, representing the manufacturing community. As manufacturers march toward building 2.0 hardware and software systems, at the same time, ranked choice voting is growing in popularity in certain areas of the country.

When I read this agenda item, I was immediately thinking of the caveat that the EAC has provided to add 2.0-compliant components to 1.0 or 1.1-certified systems, and in that use case, was there a request to, hey, I have this 1.0 modified system. The manufacturer is offering a module that assists with ranked choice voting. Was that the use case that you were thinking of, or is it something different?

CHAIRMAN HOVLAND:

And again, anyone can correct me here if they know more. At least my awareness, this has come up in a few different flavors. Some of this has been, you know, again, this -- you're correct. We've seen ranked choice voting expand in the country, more

jurisdictions having that, and so I know I've personally heard both jurisdictions ask about this because of how their state maybe implemented the VVSG and the New York example that Kevin highlighted earlier is certainly, you know, real for a lot of places and how they deal with that.

But then the other example is that, you know, someone who provides that software wants to be able to say to people, hey, you know, this has been tested by the EAC, or this has this stamp of approval for sort of credibility or comfort purposes for the jurisdictions, you know. And again, we have certainly expressed that, you know, anyone who is working with an existing certified manufacturer could certainly put that in as a modification. I haven't personally been asked it on the 1.0/2.0 transition topic.

Any other thoughts?

[No response]

CHAIRMAN HOVLAND:

All right. Oh, should I auctioneer this one?

No, we will move on to, again, you know the one that we have talked about a lot today, and I do know that it is late afternoon, but I want to go back to end-to-end verifiability and have a little bit more of a conversation about this, again, included in the 2.0 standard. Candidly, since that adoption, we haven't made a ton of progress. At the last meeting here, we did have a subcommittee

created around that. That had a few bumps. There was a little thing in 2024 that happened, a presidential election.

So, again, haven't made maybe some of the progress in that area that we would like to, but we wanted to use this time and some of the presentations that we've seen earlier to try to focus the conversation on a path forward. What are those things that we need to be thinking about? What are the biggest challenges to moving a certification standard forward for this technology? And particularly because we do have, I guess, the parameters of a subcommittee for this area, should we provide a more specific charge for that entity to better inform this body?

That makes Camden comfortable when I acknowledge that a FACA subcommittee is advising this body and not the EAC. See, doing my job, you're welcome.

[Laughter]

CHAIRMAN HOVLAND:

But, you know, again, I think, given the conversation, given the technical rigors of this technology, you know, it is not -- I think we recognize the challenge of it, but also, you know, recognize that it was in the 2.0 there was a commitment to that, and we want to identify the best way forward. And so I certainly would welcome thoughts or conversations on what are viewed as roadblocks or

challenges and what suggestions there might be to identify workable solutions here.

MR. SKOGLUND:

Kevin Skoglund, representing IEEE. So I was on the cybersecurity working group for VVSG 2.0 along with Josh Benaloh, and when we talked about the E2E verifiable sections, you know, one of the concerns that we had was, how is a VSTL going to test this? The VSTLs are supposed to do compliance. How in the world will they do that? And we kicked that around, and ultimately, what we came up with is what you see in the VVSG, which is we try to get other people's eyes on it to get sort of a peer review. And so, you know, the best we felt like we could do is it has to be available for, I think, two years so that it can be publicly commented on, and then it gets some kind of an independent review because, you know, there's maybe two dozen people who are able to really vet this technology and really say that it's working according to spec or not.

So that was kind of the approach we took at the time, and maybe that was right or wrong, but that was the concern was, you know, how do you test this and have VSTLs not have to employ these experts?

COMMISSIONER PALMER:

So, Mr. Chair, I guess my question is, is either through a committee, right, or through a committee that was sort of laid out in 2.0, you know, identifying some folks that can work toward those principles would seem to be the logical conclusion. That's sort of what 2.0 envisioned. We don't want things to get stale, and we want to keep moving forward, and so there's individuals that have the knowledge, and there's different thoughts on the principles and protocols, so we want to get those down in, you know, in writing or some sort of advisory to the TGDC. I think that is what the Chair is sort of thinking about. And who could we put on that sort of committee? And how can we get that advice to the EAC?

CHAIRMAN HOVLAND:

Thank you, Commissioner Palmer. And I think one other piece of that, I think, certainly that's an element. I think, you know, in some ways, thinking about some of the presentations that we've had today, you know, again, there have been multiple pilots since the adoption of VVSG 2.0, and so thinking about if those examples provide a pathway, you know, is this something that we need? You know, thinking about the layer cake example that's out there, you know, again, on some level of this, you know, obviously, we depend on our partnership with NIST, and the folks at NIST who specialize in this are a big portion of it.

But, you know, there's an element that I wonder how much there also could be a forest-and-trees dynamic. If you think about some of the ElectionGuard piece, to me, or some of those presentations where you've got the verifier, you know, you have this transparency component to that, you know, where is the balance on that sufficiency and what we need to be able to see versus some of the specifics. You know, do we need these standards to be overly prescriptive and basically say, this is how you can do this if we're going to certify it?

Or, again, is it more backing up a level, having some principles that must be met, but allowing some flexibility in how people get to that so long as, again, you hit what we were all discussing earlier as far as, you know, be counted and cast provisions, obviously maintaining secrecy of the ballot and other sort of fundamentals to the VVSG. Diane?

MS. GOLDEN:

Diane Golden. So I'm thinking, currently, VVSG 2.0 talks about end-to-end verifiability only as an alternative way to meet software independence outside of a printed paper ballot. VVSG only applies to in-person voting, live voting, not remote. I'm officially way past senior citizen age now, and I don't see in my lifetime the paper ballot train turning around.

So one fundamental question would be, why do you want more information in the VVSG 2.0 about end-to-end verifiability when the only reason it was put in there, because of the difficulty of going through the test labs and everything else, you know, technical standards about how to test to it? Why would you do that? Because even if everybody did that, they're still going to have a paper ballot. And the only reason of having that alternative there was to give poor schmucks like me some hope that we could vote in person without a paper ballot, which, okay, I've officially thrown in the towel on that.

So I'm thinking, using David Wagner's analogy of using resources efficiently, and I just think you'd be wasting resources, and it sounds like it's very difficult to do anyway, so I'm not sure why you'd want to go down that road.

I would be much more interested in having a group look at end-to-end verifiability to the point where it could make the case to cybersecurity skeptics that this is the best we can do and acknowledge the fact that we have a population of people with print disabilities who cannot ever vote privately and independently, remotely with a paper ballot. So we have to have an alternative to not just disenfranchise those people. And if this end-to-end verifiability gives you the best secure pathway of doing that, is it

good enough, and can we finally get over that hump? But that would not be a VVSG standard or a testing lab, you know, issue.

CHAIRMAN HOVLAND:

I really appreciate those comments, and I think that it leads to -- I'll pose a few other questions for the group, but as I think about sort of the questions that that raises in my mind, you know, I think, why are we having this conversation? Because it was included in 2.0, and it is part of our mission to fulfill that, regardless of the challenge of that. I think you raise a tremendously valuable point on whether or not that is pragmatically useful, but it was included, and so should it not be included? I mean, that would be a separate conversation.

But I also think that, you know, it raises thoughts about the way that we've seen it at least recently in the ElectionGuard pilots, it has been parallel with paper. On one hand, you know, you could argue, well, what's the point of that? But on the other hand, that may help build trust in the technology over time if you've had, you know, 10 years of elections with parallel paper and, you know, hundreds of millions of ballots, and they've all been verified, maybe that gets people to a more comfortable standard.

And then the last sort of thought that I will throw out into this rambling is, you know, we also have, with the TGDC, you know, one of probably the more comprehensive, dedicated groups to

election technology and a wide array of stakeholders, as Congress had the wisdom to put together here. And so, you know, there is probably value in having the conversation in this body to think about how we can contribute to this technology in the field more broadly, even if that is less applicable to the voting system within the scope of the VVSG.

Shane?

MR. SCHOELLER:

Shane Schoeller, Board of Advisors. As I was thinking about this in terms of the EAC, I think that one of the things a lot of government entities are challenged with is keeping in mind the purpose. And then, once you know that purpose, the scope. And so as you think about, you know, HAVA and the purpose that was given by it, is this meeting the purpose? If it is, then what's the scope? How far do we go with that? Where can we take this?

Because I think that, you know, when I think about anything certified to the EAC, it's not required, though, right? It's something that states can choose. For example, our state does certify, but they look what the EAC certified before they do that. But they don't have to certify what the EAC certified. So how far do you want to go down with that?

And then I think the next thing you have to look at, and it kind of goes back to component certification, too, is, do you want to

look at the threshold? Are they just meeting a threshold, or are they attaining? And those are two different things. And so I think that, as we think about these things, those things have to be part of the conversation because they're important conversations, but are they truly the purpose of the EAC? And I'm certainly not here to answer that today, but I think that has to be considered as part of the conversation.

CHAIRMAN HOVLAND:

Thank you for that.

COMMISSIONER PALMER:

Just one comment. I mean, one of the ways I'm looking at it is -- and the presentation from Enhanced Voting was very informative. I mean, when you look at the litigation over disability voting, even UOCAVA, you have ballot delivery, all 50 states, territories, ballot return in some states, some by court order. What does the EAC do? It sets standards in conjunction with TGDC, NIST. It tests. It's not perfect, right? It's trying to test to the latest technology.

And so either you set a standard or you do not. Either you test or you do not. So if it's hard, well, I guess that gets us off the hook, right, you know? So that's the purpose of the EAC, and so we either leave it as sort of this, you know, ornament on the tree, or we actually do something about it.

And, you know, I think ElectionGuard has proven that it is a product that may be growing. Enhanced Voting is growing. So what do we do in response to growing technology that's unregulated or untested?

MS. SAUNDERS:

So Mary Saunders, ANSI. I just wanted to build on the previous comments and Shane's in particular. I was thinking about it as a scope issue. If the VVSG applies to voting systems and VSTLs test voting systems, I could see looking at end-to-end verifiability provided by voting systems, and therefore, that capacity, capability has to be considered part of the certification.

But there are a lot of solutions that are not part of voting systems that provide end-to-end verifiability. There's a difference there in terms of how the EAC would address those. I think, given the presentations we heard today, I found that information about what is going on in the market really, really important and to keep up with the technological improvements in end-to-end verifiability not necessarily inherent in voting systems to be very valuable.

So I wouldn't put end-to-end verifiability as a priority for voting systems' testing or certification right now, but looking to your point to the future, 10 years down the road, it's good to keep up with what's going on with the technology, and you might then take a different decision later. So I guess it's a difference between

keeping up with the technology, being aware of what's going on in the broader environment, versus does this need to be something the EAC focuses on right now for testing and certification of systems?

COMMISSIONER PALMER:

I think we're a long way from testing and certification because you have to sort of follow the development of a protocol and the standards, you know, if there is a solution to this. So that's way in the future. There has to be a lot of work done by this committee plus like a subcommittee that we were talking about, the experts in end-to-end who can provide that guidance to the EAC. Otherwise, we're in receive mode until we feel confident that there's some sort of solution to it.

CHAIRMAN HOVLAND:

David, I don't want to miss you again. Oh, Shane.

MR. SCHOELLER:

Shane Schoeller. And the reason I mentioned when I mentioned a purpose scope is it's much easier to defend what you're doing when you can go back to your purpose. If you can't, then that's much harder to defend, especially when you're looking at the public in general, as well as people who are in elected office. For example, if I can go to our capital in Jefferson City and say, well, this is our purpose, what I sworn oath to, then they have to

address the issue. If it's more of an idea, then that's where I get into a little bit harder territory to be able to defend what I'm doing.

And so I mention that just to say that I appreciate what was presented today, too, in terms of all the information, but they will always have to keep those things in mind. And that helps us be able to go forward with either sure footing -- if we don't have that sure footing, then we go back to the drawing board and look at it again.

COMMISSIONER PALMER:

So, Mr. Chair, I'd like to actually just make a comment about the first issue you brought up regarding nonmanufacturer vendors and maybe then get some feedback. You know, I've heard it from vendors themselves, manufacturers. I mean, the concern that I had at the state level is that, is the service provided by vendors, or sort of the contractee, are they adequately serving local officials? And, of course, the state has a vital interest. I remember having a vital interest making sure all of -- you know, and the state can assist. And then all these other vendors are assisting and sort of the nonmanufacturer vendors.

Our concern at the EAC is just the reality that sometimes the services aren't up to what we would hope would be for the election officials. And because the rural and small counties are sometimes reliant on that, I don't want to just rely on hope, hope everything

goes well with that relationship, right? Is there something we can do? And we're going to research it, but that's really where my concern comes from. Is there anything we can do really to assist the states, but to assist the localities and manufacturers to raise that level of service?

MR. SCHOELLER:

Shane Schoeller again. As an election official, I absolutely do appreciate that because, especially when it comes to local entities and their cybersecurity team they hire or maybe a vendor they hire, a lot of times there's no assuredness in terms of who they've hired, and they're doing it in conjunction usually with their county commission. And so definitely you can find some real value in that, and I've mentioned that before, I think, in terms of if there's a way to be able to do that.

And I think that's where you can partner with E-ISAC, other organizations, and create a partnership in terms of some of those things, in terms of products and services that are delivered. Look who we can partner within those relationships, be able to do that because there is real value in that because, for example, a lot of times you have someone who is elected who has never participated or done anything in elections before, and they have a number of the duties. So if they have something that they can look to that has some type of standard that they can say, okay, this has been

certified, or this certainly has been approved, whatever term we want to use, that would give them greater assurance in terms of reaching out to them. So I appreciate that.

CHAIRMAN HOVLAND:

Okay. All right. Any final thoughts or comments?

[No response]

CHAIRMAN HOVLAND:

All right. Well, thank you all. This concludes our planned agenda for today. As we expect VVSG 2.0 systems to complete testing this year, we will rely on members of the committee to assist in educating and reassuring stakeholders as part of the ongoing migration process.

Each of you represent important perspectives and stakeholders in the safety, security, accuracy, and accessibility of voting systems across the country. We appreciate you joining us today and sharing your valuable insight and perspectives.

And with that, I am going to open it up for any final comments or thoughts from any of the members. Tom? Oh, sorry, the members. Go ahead, Shane.

MR. SCHOELLER:

I was just going to thank everybody with your team, with EAC and NIST both for putting this meeting together and all the work they do throughout the year, definitely appreciate it and just

the content of the meeting today, so just want to thank everyone for the presentations. I know you have hardworking team members in both camps, and so thank you.

CHAIRMAN HOVLAND:

Thank you. Tom? Commissioner Hicks?

COMMISSIONER HICKS:

Thank you, Chairman. One, I wanted to thank the staff for all their hard work. And two, this is the first TGDC meeting where we have a new General Counsel and new Executive Director, so I wanted to acknowledge both of them. You can clap, folks.

[Applause]

COMMISSIONER HICKS:

But also to know that this is very important hard work that we are doing -- that you're doing, not me -- that you're doing, not about me.

[Laughter]

COMMISSIONER HICKS:

And so I wanted to make sure that it's acknowledged because the EAC stood up two really good programs last year, the Field Services team and the ESTEP teams. And I think that this is a way for you to be able to have a real influence into what the EAC is doing, ensuring that we do move forward.

So Diana talked about not being able to vote not using paper, but I think that with our teams moving forward, at some point, my great grandchildren should be able to do that.

[Laughter]

COMMISSIONER HICKS:

And so, you know, I'm really proud of the work that the folks are doing, and I wanted to ensure that they know that and acknowledge tomorrow being that Commissioner McCormick will have been here 10 years as well.

So with that, we will continue working hard. And I want to thank you, Chairman, for giving me just a couple of minutes so I can be on the record.

[Laughter]

COMMISSIONER PALMER:

I would just thank you for participating. I think that this committee is extremely important because when we think about talking about voting systems, you know, confidence in those systems and the process of standards development testing is just vital. And so, you know, this is really where the rubber meets the road and sort of understanding the technologies available and how we talk about -- make sure we're making these systems as secure and as accurate and successful as possible under the Help America Vote Act, and that people that are watching or read this

transcript, they know that they got folks in a room that are doing their best to do that, and we value their comments.

CHAIRMAN HOVLAND:

Well, thank you, Commissioner Hicks and Vice Chair Palmer and Shane. Any other last -- going once, going twice.

[No response]

CHAIRMAN HOVLAND:

And with that, I do not need a motion or a second for this informational session, so I will adjourn this informational session, and thank you all again for your attendance. Thank you for all the presentations today. Thank you, Monica, for getting us here and making this happen and everyone else.

[Applause]

CHAIRMAN HOVLAND:

And we will be in touch. Thank you.

***

[The 2025 Annual Meeting of the Technical Guidelines Development Committee of the United States Election Assistance Commission adjourned at 4:14 p.m. EST.]

bw/cms