PLEASE STAND BY FOR REALTIME CAPTIONS.

All right everybody. We are 5 minutes now. At 11:59 I will come back and we will get going.

Sounds good. You want me to stop sharing my screen so you can do the introduction?

No. Please just stay as you are. It makes it easier., You are doing -- This is perfect.

[Silence]

Okay. We are 2 minutes out. At noon, we will turn off the waiting room and let everybody in and get going.

[Silence]

All right do you want to let everybody in so they can get settled and we will kick it off at noon.

All right. Welcome everybody to the overview of NIST initiatives on AI standards, principles, and critical AI issues come up posted here by the AI community of practice, which is part of digital.glove and the conglomerate of communities of practice. As a reminder, if you have joined just before, this event is going to work kind of similar to our others. Everyone will be muted for the entirety of the meeting. Please put any questions and comments into the chat. We will handle those with the folks from NIST. Also a reminder, this is being recorded. You will be able to find a recording of this presentation on our webpage, which is being dropped into the chat right now. As a reminder you will not be able to come off of mute. Please direct any questions or comments to the chat. This is being recorded. With that, what, then and I will turn it over to Steve Babich.

Thank you, everyone, for attending. Along with me is Krista Kinnard. We run the AI community of practice and we are glad you all can join us today. We have a really important event. Thank you for joining. We have today experts from NIST , the National Institute of Standards and Technology , who will find an overview of some of their key artificial intelligence initiatives, but I will let them get into that in more detail and specifically our experts, first is Elham Tabassi. She is Chief of Staff in the Information Technology Lab at NIST. They support U.S. innovation and industrial competitiveness by advancing measurement, science, standards, improve our quality of life. ITL conducts applied research in science engineering and cultivates trust and information technology by developing standards of information systems. Welcome. Additionally, our other expert is Mark. In his capacity he leads with industry academia and other government agencies to foster trust and emerging technology that makes sense of complex human information by developing improvements, managing technical evaluations, and contributing to standards. TR EC, several biometric benchmarking programs, and a growing number of technical evaluations of natural language processing and speech image analytic technology. His current interests are in AI benchmarking, explainable AI, and bias across the AI lifecycle. Thank you for joining. Certainly we are excited to have you both. These are certainly topics that are high interests across the federal government ecosystem and to a number of stakeholders. We will have an overview of the work and we will certainly make time for Q&A. Please do feel free to drop your questions in the chat at any point in time. We will make sure to cover those. That said, I will turn it over to you, Elham.

Thank you. Thank you for the invitation. Thank you for having us here. We are pleased to be here and talk about the NIST AI program. Very good. A few words about NIST , the National Institute of Standards and Technology . I'm sure many of you are familiar with NIST, but NIST was previously the natural national Bureau of standards. At that time, the United States had few national standards and it was typical for Americans to conduct transactions to fit together properly. That is the foyer at Baltimore city, and NIST was put together in 1901. Congress charted the creation of the national Bureau of standards. Today NIST is home to 5 noble prize winners. It is a strategic priority for NIST. As Steve said, I am the Information Technology Lab, one of six research labs at NIST. Our purpose is cultivating trust in I.T. and technology. We use the measurement and testing resources, which impact a wide range of areas of computer science, mathematics, statistics, engineering. We also have psychology and cognitive scientists on board. The area or spectrum of work goes from fundamental research all the way to route option. We work on the scientific underpinning of the technology. We also work with scientists

for applied research, how to get that research applied. We contribute to the development of technology fit for standard and best practice guides. We work with industry very closely to make sure that those standards and best practices are being adopted.

That is exactly what we are also doing in the area of AI. The area of AI needs tools and measurement to understand the capabilities and limitations of artificial intelligence technology. We establish technical requirements needed to cultivate the trust that AI systems are accurate, reliable, safe, secure. That is a very important topic these days, because while there has been major advances in artificial intelligence, it depends on the link that you click on our article that you pick up, they can talk about how great AI is and how it can raise productivity and enable more efficient use of resources, and basically it will change your life for the better. There are some that talk about the negative impact on humanity and jobs. Some even talk about a threat to humanity. The truth is really in between. That is really what we are trying to do with our focus on fundamental and applied research and standards for AI technologies. Just like any other program, just like the spectrum of the work in ITL for the AI, our work goes from fundamental to applied development of standards all the way to adoption of responsible, safe, and secure AI technology. So, what are the components of our program?

I will be talking a little bit about each of them. We have a component of the foundational research. This is to establish the needed scientific foundation for development, design, and assessment of trust with the AI. I will be going back to foundational research and talking more about this. NIST has a very broad portfolio of research going from robust advanced manufacturing to materials science, bioengineering peak we are working with all of the scientists to advance AI as a tool to the improvement of discoveries and technological innovations. We have a long history of evaluating components of AI systems. Examples include the NIST biometric evaluations. Many of you have heard about facial recognition technology. Currently we are working with the national cyber security Center of excellence in assessing AI vulnerabilities. Testing is our middle name and we work with standard developments. We developed tools and guides in the areas of AI. We are focusing on data metrics and testing for AI. Also engagement. Scientists, engineers, technical experts working in the area of AI, but also psychologists and lawyers. AI is increasingly a multidisciplinary area of research and we want to make sure that when you are talking about trustworthy and understanding what constitutes trustworthiness, all voices are being heard and everybody has a seat around the table.

So, what are we exactly trying to do? You all know that there has been many different high-level principles for trustworthy AI. Many countries, I believe something about 60 countries have signed onto that. Also other entities in the community of interest at GSA are also working on principles of trustworthy AI. All of them are being used. The documents, when you look at them, especially going back and talking about OACD, all of them are value-based statements and rightly emphasizing the importance of human centric, respecting privacy and individual rights. While there are many of these documents, there is also a lot of overlap among them. The challenge and opportunity for us as a community is to get those value-based high-level statements and translate them into technical requirements that can be designed, developed, and be used for assessment of AI systems. What are those technical requirements? What is accuracy? Everybody wants the system to be accurate. There is a lot of activities going on in the development of more accurate systems, and also methods and mechanisms and ways to measure accuracy is much more advanced. Beyond accuracy, it is also important to make sure the system is secure to different attacks and manipulations. Many of you have seen some of these examples of, I think, a paper by Microsoft a few years ago, by putting a Post-it note on a stop sign, the AI system was confused and could not recognize it as a stop sign, when the human brain can easily see it as a stop sign and realized that there was a Post-it note. Security is an important issue and we have a research program event that. Robust and general flexibility of the algorithm that was not seen during the training. How the AI system is going to perform in operational settings in the real world setting, and how closely it is going to follow the performance that was measured during the training is another component of trustworthiness of AI. We want AI to be explainable. There are a lot of applications and use cases that there is a need to explain how the algorithm came to the prediction or the decision or the recommendation that the algorithm is putting forth. That is something that Mark is going to talk about more today. Biasing AI is a topic of interest that we have all heard and seen a lot of articles and talk about the issue of the bias in AI. Reliability, privacy, and several other are also technical requirements of AI. One of the things that we will be working on follow up to the workshop we had on August 6, is to come up with this list of technical requirements. What constitutes trustworthiness? And get agreement from the

community on that. It is only after we know what it is. When we know what are these technical requirements, the next step is to work on the vocabulary terminology and have a shared understanding of each of them. So bias and explain ability, these are things that can mean things to different people. We can get the whole community on a shared understanding as to what we mean by bias and vulnerability, and what these touch points are in and AI lifecycle. It is only after we know what it is that we want to measure that we can move on how we measure them and develop metrics and measurements and procedures for assessing these components or technical requirements for trustworthiness.

So, I thought of sharing a quick overview of happenings in the summer of 2020. I didn't put here that we launched a public-private partnership in understanding what constitutes trustworthiness. We had a workshop on August 6, and it was a half-hour. The recording of that workshop is on our website if you want to go and look at that. The idea was going from principal to practice, to build a community working on getting this value based high-level principles, get them into technical requirements that can be designed, developed, and processed her AI systems. As I mentioned, we also have a research program around bias in AI. We had a workshop on August 18. In the morning, we focused on the issue of bias in data. In the afternoon it was around bias in algorithms. We have been doing a literature survey, and again the recording of the workshop, in addition to the preview of the material, are all on our website. We are working on a summary report of the workshop, but it is a little bit broader than just a summary report of the workshop. We reflect on some discussions in the workshop. Also, I give a survey of the use of the term bias in different literature. Security of AI, this was the first research project that we initiated. We put terminology and Taxol many out. It went through a round of public comment. We received really robust comments. We are finalizing and hoping to get it out by the end of this calendar year. Explainable AI, as I mentioned, it is one of those components of trustworthiness that we have built a research program around. I want to say that this is one of the more difficult ones to tackle. What we mean by explainable, and is it always needed? No. Sometimes no. Things that recommend which movies I can watch, or that I can watch based on the history of by removing watching Emma I probably don't care much about it being explainable. If you are using AI and applications such as hiring or a loan application, or even medical applications, when there is a way that you can decide that there is a tumor in the MRI image of a brain scan, then you probably need it to be explainable. And what explainable is useful. If you are giving it to a technical expert versus the example of the medical imaging that I mentioned. Explanation to a patient, to an insurance company would have different -- [Silence]

I think we lost audio. Kenny will hear me?

Yes we can. Elham , it is Gabby, I am privately messaging her now. Thanks, everyone, for bearing with us. Just a minor technical glitch with Zoom peer called on one moment. Mark, why we try to get Elham back online , can you maybe jump in?

Sure, can you hear me okay?

We can.

Okay, great. I guess I will -- Our purpose of coming forth today was really to give an overview on what is going on at NIST in AI . We want to give you some of these details of area of research and we are hoping that we can take a deeper dive in the future. I would like to talk a little bit about the areas of work that we are doing in our division. We have a very strong history in measurement, evaluation and the involvement of standards and the focus on human action behavior and characteristics. These technologies are those that deal with data that is an audio, text, images, and video. They seek to understand that the information is contained in the data. The sampling of the evaluation projects that they run includes things like speech transcription and translation and understanding. Natural language processing and speech and search, I'm sorry, search and retrieval, we have some work and image authentications and forensics and then a lot of work in biometrics with facial recognition. Then in the video world we do a lot with person and object and detection recognition. All of these technologies are many of these technologies that are being developed through this evaluation we see as forming the essential building blocks for meaningful AI. So, building on this history and the expertise, we recently formalized a list for AI formulation. The goal of our research is to support the advancement and deployment of measured AI

technologies. NIST conducts R and D of measurement methods in the emerging and existing areas of AI. We do this for various classes of AI applications. The goal is to publish technical reports and to facilitate the measurement and standardization processes. As well as facilitate the adoption of guides for AI technologies and they mature and find new applications. What is interesting here is that AI system evaluation is very different, and it assumes the traditional evaluations of typical machine learning algorithms. It is also very difficult from the typical component evaluations that NIST has conducted in the past. The experience gained through those many years of running those in managing those evaluation driven research projects is paving the way now for meaningful evaluation of AI systems. We were just beginning to talk about AI explainability. We started to think about explainability in AI systems sense, in many ways, at its core, this is a measurement science challenge. In the areas of explainable AI, we set out to start the conversation about what it means when we want to claim that a system has a feature of explainability. A large part, this is a terminology and taxonomy department. We standardize the areas of agreement and disagreement among the AI community regarding AI terms for explainability's and concepts. To do this, we released a NIST --

---

Can you hear me?

I can peer do you want to pick back up?

Aye, sorry about this. I am troubleshooting. Maybe, maybe, I am sorry about this. I am not sure, do you want me to pick up? How far --

---

If you want to start sharing your slides again, I think you were, let's see, yes, you are on this page. Mark, how did that sound. Did you cover items here?

I think she was on the sled before this, finishing up. And one before this. That is where you are finishing. One more slide. You were finishing up on explainable AI when you cut out.

Okay. If you want to continue, Mark, either way, that, if --

If it is okay with you, I will just go ahead and finish talking about explainability and then he can pick back up. Does that make sense? Thank you. So, the NIST , and the four principles of explainable AI that we released was done in an effort to document the areas of agreement and disagreement on these concepts and terms. In a nutshell, the principles paper talks about the principle of requiring the company evidence with each decision, requiring the evidence that is presented accurately represented the processes they used to come to those decisions, and make sure the evidence was understandable or interpretable by the intended user. And the final principle was at the evidence would only be generated under circumstances that the systems was designed to operate. So, we started in this area relying on the experts in biometrics, trying to develop these principles and then expanding it out to other domains. Every time we talked and individuals, we learn something that we modify our design and concepts. That is why getting the public involved was so important to us. We put the paper out for public comment. That period has closed and we are going through the many comments received. It will likely lead to a second release of this paper, and we will probably go through another round of public review. The timing of that is still to be determined. I do know that we are one signature away from being able to announce an opportunity to get together and talk about some of these. If you are interested in explainable AI and these principles, be looking for that. That will be an opportunity soon. Our goal, again, when we come to agreement on a set of principles, NIST will be able to provide some insight into the challenges of designing and measuring explainable AI systems. That was an evaluation and AI expandability. Another area of work coming out of our division that is less mature than the other areas, but we have begun investigating from a cognitive science point of view how users form their trust decisions when it comes to AI decisions. Here users covered a wide swath of people. Developers, employers, people affected by the decision, people using the decision. While this starts with terminology, what is user trust versus system trustworthiness for example. I think, again, it is another fruitful area that we need to go down. There are other NIST efforts that measures AI system trustworthiness through the study of accuracy, reliability, security, and explainability, but the user trust program will support the widespread adoption of AI, by studying how, when, and how much trust humans place in AI systems. It is the user and their choice to trust the AI system. The point is to understand and identify end-user

challenges for understanding and establish the measures of user trust. Again, the final goal, once we have this all done, would be able to incorporate user trust measurements and thoughts and ideas in the system design process. We do have a paper that is going through internal review. When the concepts are finished evolving, we hope to be able to release our initial thoughts in the near future. The final area that I was going to touch on very briefly -- I think Elham already talked about most of it -- Was AI and bias. We want AI that is free from bias. Is important to avoid bias and prevent discrimination. As NIST works to develop AI systems that can be trusted, it is critical to develop and train these systems with data that is unbiased, and to develop algorithms that can be explained. The purpose of this project is to understand and examine and to mitigate bias in AI systems throughout the development lifecycle. We have a team that investigates bias. There is a large public workshop, virtual conference held back in August. That did bring together people from academia and industry and other government agencies. We are looking forward to a final report coming out soon. We have teams in all of these areas, and as I said, if there is interest in people would like a deeper dive, we would be happy to go into any one of them in the future.

Thank you. Again, I apologize for that. So, these were all of the building trust in AI algorithms. We also do have other research area on novel computational paradigms for AI. As we all know, the major share of the advances in AI are due to computational resources and GPU, and the availability of data. The advances in architecture that have been predictable for decades are now slowing down. One of the machine learning applications remain elusive. Are mathematicians and physicians are working on how to look at new computational paradigms, beyond the Boolean algebra, and layers of the neural net, as well as novel technologies, such as a spike neural net. That is one area that we are working on, new exotic hardware, but also the analysis and benchmarking and comparative analysis with traditional hardware.

We talked a lot about the programs that we are doing, and the new research areas that we have built for trustworthy AI. I do want to say a few words about our past work that are AI and machine learning has been going for a long time, not only as a tool for researchers, but also as a tool for data and evaluation. This is one piece of data from MNIST. This is the standard test data set for evaluation and assessment on benchmarking of image space learning algorithms. It is a set of handwritten characters. And Yann LeCun, one of the fathers of deep learning, here is a quote from him about the use of the MNIST. We are working on, we are hoping to be able to do more of this type of open public data for the advancement of the ad technology.

Mark I'm sure talked about the evaluations, and again this is something that we have a history on that. I mentioned TREC. Many of you have seen Watson that appeared on Jeopardy. You may be excited to know that the idea of the Watson was forms at one of the TREC conferences , and the earlier version of that was tested at NIST. We have some history of evaluation, and we are building a program around what evaluations of the AI algorithms or AI systems should look like or want to look like.

A few words on the coordination activities. That was also one of the pillars of the NIST program. The NIST director is a member of the AI select committee that is chaired by OSTP NSF and DARPA. Then there is the NSTC, the national science and technology Council . They write the strategy planning and develop strategies for AI. That gets headed into networking and information technology, working R and D, and the working group. And these representations of all of these, machine learning and AI subcommittee, Mike Foster is one of the cochairs of the MLAI subcommittee. Many of us sit and contribute to the NITRD AI interagency working group. I work as the standard coordinator, and that is under the NSTC plan that we developed in response to the executive order on maintaining U.S. leadership in AI. We were tasked to develop a plan for federal engagement development of AI standards. I will be talking a little bit about that in the next slide. I just want to say that our colleagues at that national security commission of AI. I am sure you have seen the recommendations, and the final recommendations and report is expected March of 2021.

Talking about the USG AI standards, that was a role that was recommended in the plan that we developed as a response to the executive order, and the job is to out reach and connect with all nonfederal efforts relating to AI standards development. Understand what is going on, what are the needs, and maybe come up with a list of the priorities and strategic involvement in standard development. Many of you know that prior development in the U.S. is bottom up, private sector and industries are on the forefront of the development of standards. But USG

and federal agencies have some role in helping in the development of the standard. We facilitate ongoing discussions between public and private sector, and look for opportunities to strengthen the leadership of the U.S. in standard development, including contributing what we learned from our engagement and research program on bias and explainable AI and security of AI to the standard development processes going on.

Here is some of the policy documents developed in 2019. The AI progress report that NITRD put out. The AI research and development strategy planning that was put out, and the plan that we developed as a response to the executive order about federal engagement and developing technical standards and related tools. We have contributed to all three. With that, I'm going to stop. I apologize for the technical difficulties and I open up the floor for questions for me or Mark. I think I will stop sharing my screen as well pick

---

You can leave it up. No problem. If anyone has any questions, please do drop them in the chat. They are here to answer anything that you might have. I guess one question, Elham -- To keep aware of various activities that are happening, do you have a listserv that we can also share to the AI community of practice?

You do have a listserv, and if you go to our website, it is at the bottom. I will send it to you so you can share it. We would be most happy to share.

Thank you so much. We do have a question here. I think you mentioned that evaluating accuracy of AI was an area with some maturity. Do you have a reference you can point us to?

Not off the top of my head, but basically, the false positive and false negative rates for any of the classification systems is, more or less, a mature field. The subcommittee that are working on the standard divisions of AI is also looking at that, and they are talking about false negatives and false positives as measures of accuracy. I will follow-up with a link to ISO activities on accuracy, and some of the Academy papers. Mark, if you want to add?

I think the only thing that I would add is that, in the sense of having some maturity in measuring AI system accuracy, we have some experience in partnering with other agencies and programs in this area. I would also like to say, I guess, that there are nuances in evaluating and AI system, such as, you know, not having ground truth or a golden reference answer to some of the test data. There have been methods through other evaluation methods at NIST -- We have to overcome those challenges. The maturity is there in structure and format and infrastructure , not necessarily -- We don't yet have it I would love to have, which is a testbed of bring in any type of AI system you would like and we will be able to evaluate it in this harness. That is something we are working towards.

Great. One thing I did want to comment on, it things like a lot of people are interested in the links you were talking about and the recording and the slides. I just wanted to let everyone know that we will be following up and getting all of the resources they have been talking out and we will send a follow-up email to the listserv with a link to the recording, the slides, and all of these links that Elham and Mark are referencing .

Thank you for that.

Yeah, of course.

Any other questions, please do drop them in the chat. I know that Elham, Mark, Christa and I, we have talked about having them come back and go more deeply on these issues. I suspect that will gather some interest as well. We've had that discussion.

We are super grateful for the opportunity. One thing I have to mention, and I am sure Mark also talked about this, that NIST, as you know , is a nonregulatory agency. That is a very important factor in how we work and the engagement that we have with the industry, academic, and the whole community. All of our documents and all the work that we do, we really encourage, and we are grateful for, the community review and comments on our documents to make them better. Any opportunity for engagement, and getting your input and comments on our documents, we are super grateful. We look at them very carefully.

Yeah. I think that is definitely something we can do going forward, is make sure we get the message out to the AI community to make sure you are getting the reach and the visibility that you are looking for. I'd be happy to do that. Any other questions? All right. Okay. We have one. Okay, we have a couple more coming in this one. The question is, is there any existing AI overlays, framework, or other consumable material to support integrating the federal privacy and security listed in the AI --?

This is a really good question. Many of you may be familiar with the cybersecurity framework and privacy framework. Those frameworks were developed for a risk management approach for cyber security and privacy. They were also developed with some of the AI and AI applications in mind. They could be leveraged for cyber security or privacy for AI, and we are working very closely with those things, and building on top of that. Ultimately, if we talk about what constitutes trustworthiness and what we want to measure and come up with the metrics and measurements and mythology for assessing those for trustworthiness, then we can start working on a risk management approach to AI. This is something that we have our eyes on and we want to work towards that. I keep talking about trustworthiness, but the other side of the coin is risk, right? Accuracy is an aspect of trustworthiness. Errors are a risk. Security is an aspect of trustworthiness, while vulnerability is a risk. Bias is a risk, and the trustworthiness aspect on that is being objective and free from bias. When I say that we work on technical requirements for what constitutes trustworthiness, another way saying it is a taxonomy of risk. When we know the risks or we have a good understanding of how to find them, there are metrics and measures to assess them, and help make standards and guides of integrating them. These are part of the risk management approach on AI. Where we work towards that, there are certainly other frameworks, like cybersecurity frameworks and privacy frameworks that could be leveraged in the process of developing risk management three.

Thanks.

Our next question, is there any research going on to others and the cognitive impact on AI as we start including more of it in our day-to-day systems? For example, how it would change user workloads and their cognitive processes?

This is Mark. I will jump in here. In our division we do have a group that focuses on the human factors of I.T.. They champion the human experience in I.T. While we don't have active work in this area, it is an area of discussion and rife for future involvement. If there are people out there that are working here, we would be interested in partnering.

Great. Thank you. Can you talk about identity for AI? How is it secured? Does it play to trust? Anything you are aware of?

Can you clarify what you mean by identity? Is it identifying people --

---

Maybe if you get a chance to drop something into the chat, or if you want, can we allow them to come come off of Butte for a second?

It looks like he is talking about fake identities or my identity as Krista Kinnard and I log into an AI system, is that being managed? Or if a fake identity logs in, is that what you are talking about? Botts. So like fake people or fake things.

Right. So, and Mark can talk, Mark, please feel free to answer this. We all have heard about deep think. And neural networks that can simulate images. They build the right probability distribution functions and sample from them. They can generate face images of the people that don't exist, but those images look very real to our eyes, to humanize. That of course can have issues and concerns about identity, and how, for example, my face can be stolen and be morphed into somebody else's, and be able to hack the system. So, the topic that you are referring to goes from, you know, morphing images intentionally, trying to break into the system. You probably have heard about the research at CMU where they come up with eyeglasses. They can build 3-D eyeglasses that people can wear and full and AI system and still a known identity. These are all under the category of the

vulnerabilities of AI systems. Some of them we are trying to address as part of the secure AI program. A lot of the issues we face are also being studied in Mark's division.

Great. Mark, anything to add? Or should we move on?

I don't think adding anything is necessary at this point. Again, the goal of a lot of the work that this does in this space for facial recognition and understanding involves the image authentication, video authentication, is to measure technology performance, not to prescribe solutions.

Helpful. Thank you. As a follow-up to the question around research going on to understand the cognitive impact of AI, follow-up question is, how can we get involved?

Mark?

Yeah, so, as I was, what I was trying to say, these are areas that we are discussing. We talked about the strategic planning of the actual group that works in the human factors area, this is a topic that has come up. We do work in AR and VR, and also augmented reality and virtual reality, and there has been, you know, conversations about how such technology has been used to modify people's cognitive capabilities. If we are going to expand into these areas, we would do that if there was an identified need, and I am looking to get involved with others, if others have interest in this area, and have a problem, especially a measurement science problem, the group would be happy to contribute and collaborate. We do not have, let me be clear, we do not have an active area of research in this space right now but it is something we have discussed.

Great. Thank you so much. Appreciate it. Another question, following on to the security question, are there existing guidelines to integrate security into dev ops for AI development?

Nothing that NIST has developed yet, but, so, a lot of our research, as you remember, I think my third or fourth slide, was going from foundation to apply standards to adoption. By foundation, we start at the terminology and taxonomy. That is a great question. We have not developed any of those items at paragraph the top of my head, I am not familiar, or haven't heard of something that I can mention right now about those. There are some algorithms, that sorts a checklist out by UK, Canada, and AI global, I believe, or even IBM. You may look into that. They may have a section addressing that. But they are all in terms of sort of a checklist.

Yep. Yup.

Yeah.

And we are looking to have, I believe it is on our list of events to come. We are looking to put them in front of the AI community of practice. Krista I think you want to say something related. I am not sure where you are going to go pick

---

We did have an event recently with the dev ops community of practice, and actually the RPA community of practice where we talked a little bit about this concept now coming out called AI ops or ML ops. It is starting to embed AI and machine learning in the dev ops process, because the development of AI solutions, right, they are very iterative in nature. It is different how you would deploy these. We can circulate that. Is available on her max page. If it is not there it should be. We will also send that out as one of the resources that we sent him a follow-up email. There was a really good question, speaking of RPA. There was a question about, so, these frameworks that you are building for AI and the way you were thinking about AI, is that also applicable specifically to RPA, so robotics process automation, or more broadly to different automation and technologies as they come out?

That is a very good question. A lot of work that we are doing right now is, we call them, borrowing the standard lingo, is horizontal. There are things applicable to AI regardless of the particular technology and specific domain. We understand that there is a limit on how far we go, just talking about horizontal and use case and domain. We think it is really important to settle that foundation. After that, we have started thinking about and connecting to

the different communities to build vertical. So, you get to do the explainability we are talking about, and the importance of each of them. The specificity for each of these for the healthcare community, versus autonomous vehicles, versus free stress ignition pick so, now, what you mentioned. At this point, we are thinking about horizontal and domain specific diagnostics. Yes, we are thinking about building communities around vertical pick I hope that answers the question.

That's great. Appreciate it. Another question, are there any decent RAI subdomain playbooks currently collected. What they have found so far is very generic. We are actually, Elham and Mark, maybe you are aware of some things as well, but one thing we in the AI portfolio have pulled together and we are looking for approval supposed to set to the federal government is a perspective on how to think about AI capability building. So, this is something we are anxiously looking to provide to all of you and we are hoping for, early in the new year, a lunch of that. That is one thing I want to make sure that we let the community know and be aware of.

That is great. A lot of these activities are happening in different communities. Events like this and bringing different groups together is really important, because we can all learn from each other, and complement our efforts, and be more effective and efficient.

Fantastic.

We have a lot of questions, are there standards of transparency of training and test dating that a researchers with a conflict of interest.

I was hoping to see if I get a chance to talk about actual data. Was having discussions to talk about data. Data is really important. Documentation about what type of data was used for training, have there been any checks for bias. You know, the providence of data, the governance of the data. These are already important. You use the term transparency of data. I assume by that, you mean sort of the documentations on what data was selected, how data was collected. What tests have been done on data. The size of the characteristics of the data. Extremely important topic. I believe they have done some work on that. There is a data working group and they had some documents that have some relevance, not exactly answering all of the questions. Some work has been done but a lot more needs to be done. That is my personal assessment. But it is a really important topic.

Thank you so much. We have another minute, so we probably need to wrap up. I think we dropped a link about our upcoming summit. Before I give an overview of that, I want to thank Elham and Mark so much for your time and effort. The work you are doing is clearly important. We look forward to having you join us and provide details on the various efforts you have underway. I know it is just an overview. There is certainly more to cover. Thank you both again for your time. I really appreciate that.

Thank you for having us. I apologize for the technical difficulty on my part. I am grateful for you guys and Mark for picking it up. I hope everybody enjoyed it, and it was useful, a good one hour of your day. Thank you.

Thank you. So, yes, coming up, I think it was dropped in the chat, but, coming up on November 19, from 2:00 to 3:30, the U.S. tech transformation service, we will be hosting our AI summit and webinar focus on some of the work that is happening across government related to AI, so the tool resources and projects that are already resulting in some impacts. Please to join us. I don't know if you want to drop the Lincoln or if it is in there again somewhere, but feel free to register via that link provided.? Again everyone. We are at 1:00. We will see you next time.

Thanks, Steve.

Goodbye.

[Event concluded]