President's Council of Advisors on Science and Technology (PCAST)
Public Meeting Transcript
May 20, 2016

Welcome from PCAST Co-Chairs

>> JOHN HOLDREN: Okay, good morning everybody! Could I ask the PCAST members to take their seats? And we will call this PCAST public plenary meeting to order. It is a pleasure once again to welcome the members of PCAST, the members of the OSTP staff who are with us, and the members of the wider science and technology community in the public who have joined us both in person and on the live stream on the web.

As usual, we have a full schedule this morning. As with forensics, near-earth objects, crypto currencies, and that is reflective of the full schedule that PCAST has had throughout its tenure in the Obama administration, and that in turn is a reflection of the extraordinary degree of engagement and interest by President Obama in matters of science, technology, and innovation. I can tell you that nothing is slowing down as we go into the last 36 weeks, and now maybe at the beginning of next week now, 35 weeks of this administration. The president is determined to advance as far as possible as many of his signature initiatives as possible, and that includes the many that are in the science, technology, and innovation domain. And certainly PCAST has a number of studies underway that we want to bring across the finish line before the end of the term. With that said, let me turn without any further ado to my PCAST Co-Chair Dr. Eric Lander who will add his welcome, but then will turn promptly to the topic of forensic science. Eric?

>> ERIC LANDER: John, thank you very much. I want to welcome all the members of PCAST in the room and everyone who is and will be watching on the web. There is a lot still going on at PCAST. After today's meeting we still have four more official meetings set for this group, and the work is not letting up in any way. I'm very grateful for the members of PCAST for their active engagement in at least three ongoing studies and a few other projects. So it's just great to have everyone's full participation.

Forensics

>>ERIC LANDER: I wanted to take a moment and update everyone about the project that PCAST has been engaged in on forensic science. It's a project we mentioned before, and we're now nearing completion of the project. We're in the process of trying to write up a report on that. And I wanted to at least describe a little bit of the motivation for it, the work underlying it, and directionally where we're going. We still haven't reached any conclusions yet, but I think it's pretty clear where we're going in terms of the questions that are being asked. So forensic science in some sense is a very old discipline; folks recognized more than a century ago that different types of scientific and technological evidence could be useful in the criminal court systems, fingerprints being an old example but many different types of patterns that might be encountered in the crime scene might be used to connect the evidence at a crime scene to a particular individual, a perpetrator, in some cases a victim. There were many different technologies that were proposed early in the 20th century. There were early forms of lie detectors that were offered up. And these lie detectors really lacked much scientific foundation. And the courts in an important decision, federal appellate decision, began to erect some standards as to what it meant to have scientific testimony in the courts. So there's been a parallel development of

methodologies, and considerations of how to evaluate whether those methodologies are appropriate for use in courts. A real watershed moment occurred in the late 1980s and early 1990s with the introduction of DNA fingerprinting technology, based on the scientific recognition that the human genome was variable between people. That some regions of the human genome were quite variable, had many different alternative alleles, different forms of the DNA. It was possible to find in medical research labs, if you took DNA from different people, you could observe different patterns in different places from the human genome. In the late 1980s this began to be introduced in courts as a forensic matching technology. You find some blood on a potential perpetrator and match it to a perpetrator or victim. Or you might find blood at the scene of a crime and match it to a perpetrator. It began to be introduced. And very interestingly, despite being the most powerful of the forensic technologies ever developed, in its maiden voyages, it encountered some rough seas, and in some notable cases DNA evidence was excluded from the courts as being inappropriately practiced. This led to a tremendous effort to set standards for the use of DNA evidence and within a couple of years through work of folks notably at the FBI's own laboratory, DNA becoming a gold standard. It taught us something very important. It taught us that even the most absolutely superb, basic science still has to be practiced reliably to be useful in a forensic setting. And this combination of scientific thinking and then real forensic work to set standards and assess reliability together produced an amazing gold standard that is used in the courts today, the DNA analysis of single samples, unmixed samples that is remarkably reliable. But the minute we had a reliable tool, you could start using it to go back to other cases and ask if there were any mistakes made. This became the next real revelation in forensic science that began to gather some steam in the '90s, but really it has been in the last decade that it has become clear that DNA evidence has made it unambiguous that there are wrongful convictions. In fact people have been sentenced to death wrongfully, and we know this now because we can see in many cases evidence where a bloodstain was said to match someone, but when you looked at DNA it clearly did not match someone. But it often doesn't match them. It often matches someone else, the real perpetrator. So we have two wrongs here. A wrong to an individual who has been wrongfully jailed, and a wrong to society, leaving a true perpetrator on the street. Both are serious issues in regard to justice. The ability to know that we make mistakes is essential to science. Science is about the ability to detect mistakes. Nothing is perfect. What sets science apart from other activities is we know it, we embrace it, we measure it, and therefore get better because of it. So it has provoked some real thinking about how did the criminal justice system get things wrong? Well in more than half of the cases, roughly half of the cases, the evidence included scientific forensic science evidence that contributed to a conviction. And because it made a claim that we now know is wrong, we know it made a false claim. How did that happen? So that's pointed to problems with technologies like bite marks or even fingerprints or hair analysis. Or other types of things. And what it provides is a great opportunity to increase the quality of forensic science. The National Academy in 2009 issued a report from an NRC committee that described what only could be said to be deeply serious problems with forensic science. That report concluded there were issues with the underlying scientific validity of these areas and it made a whole series of recommendations. That report has been tremendously important in focusing people's attention on the problem. The Obama administration responded by creating a National Commission on Forensic Science, which reports to the Attorney General and is coordinated with NIST, the National Institute of Standards and Technology, and this national commission on which one of our own , Jim Gates, serves has been an important forum for discussions for many things; standards for accreditation. There are discussions going on right now about discovery procedures with regard to forensic science in criminal cases. What information should be turned over to each side, etcetera. There are many important things happening there. In addition,

something called the Organization of the Scientific Area committees was established by NIST where something like 26 different areas have committees where forensic practitioners primarily are trying to improve best practices across their 26 areas. And continual improvement of best practices is a very important ongoing thing. We applaud the activity that was launched by the administration. But in reviewing the area at the request of the President, our job was to ask what's not happening enough. And the one area that we've really focused on is the question of the fundamental definition of what does it mean for a forensic science method, and in particular a pattern comparison method to be based on reliable principles and methods for all possible or purported scientific The law requires that for evidence to be introduced by an expert in a federal court, it's called rule 702 of the federal rules of evidence that we've come to learn, it must be based on reliable principles and methods. But the law doesn't define reliable principles and methods for all possible or purported scientific or technological methods. It gives those terms. What we've set out to do in a way to be helpful to the federal courts, to prosecutors, to defense attorneys, to forensic scientists, is to give a clear, crisp description of what it means for a forensic pattern comparison method to be based on reliable principles and methods. Forensic pattern comparison is a subset of metrology, the science of measuring and comparing things. And happily in this case, metrological sciences, the scientific community has a crystal clear sense of what it means to know when something is reliable. And of course it depends on empirical measurement. You know something is reliable because you try it and it gives the right answer with high probability. There is a clear set of guidance there. One of the things that PCAST is set out to do is to try to explain very clearly what those standards are in a way that all the parties in the field can use. They are important because they control admissibility in federal court. In addition, what we've tried to do is understand how those principles apply to some areas, some examples of forensic science methods. Here we really first sought to get the input of the whole community. So PCAST was unusually vigorous in gaining input. We've held a large number of meetings, probably 20 meetings either here in public sessions, or subgroups of PCAST having phone calls with people or our staff doing deep dives to truly learn the literature. We took the unusual step of making a call on the web, asking anyone to offer to us their input on the questions of reliability of methods, to point us to papers in the literature that would point to the reliability of different kinds of methods, to offer us advice in any other way. And we received 74 replies on the web, I believe and they point to something like 399 different scientific papers, which PCAST has reviewed and in a few cases is still working its way and reviewing so that we with could learn about this subject thoroughly. And we are enormously grateful to all of the individuals and groups who have taken the time and trouble to write to us and send us their thoughts. Some of them are very extended and lengthy thoughts. All of these will be made publicly available together with the report. All the references we've pointed to can be made publicly available. We've also reached out to federal judges and put together an advisory group of federal judges who have been able to provide us advice on what the law actually says and also how to be able to bridge the communication divide between scientists and judges and expressing clearly what the scientific definition of reliability means in a way that it would be valuable to folks in a courtroom. So we've done all that, and what we will attempt to do, and we're still working our way through it, and so I can't report anything definitive here, because we're trying to be extremely careful looking at the literature. But it is to apply those guidelines about what constitutes reliable principles and methods to a number of different areas, as an illustration of the kind of reasoning that is necessary. I don't think it is going to shock anyone to say because the National Academy said it loud and clear, there are some forensic science methods that do not have foundational validity. There simply isn't evidence of them. But we're going through carefully and we'll make some decisions about how that is, but it's important to know, because in many cases it may be possible to get foundational validity. Remember, foundational

validity doesn't mean perfection. A method doesn't have to be perfect. But it does require that its error rates are known under relevant circumstances. If you can't actually tell me, well there's a wonderful quote from a federal case U.S.V.E. that someone pointed out to us about smiles. To say that two smiles match. Are we talking about a general smile or a Mona Lisa smile. If you don't know the details of the matching rule for smiles, you don't know if that's a meaningful statement or a meaningless statement. For a whole lot of different reasons, it's important to bridge this communication gap. We are really, really admiring of the work that has been going on so far within the administration on it. And we really see this key issue that everyone has pointed out to us, for the need of the courts to be able to clearly define this admissibility criterion as a place for us to apply work. Our report, hoping that before the next meeting is completed we'll be able to bring it to public discussion either at our very next meeting or if we get it all done, perhaps at a phone call meeting. We'll see how it's all progressing. It will be a useful contribution to what has been an important ongoing process. I should really say that the higher the quality forensic evidence that we can have in courtrooms, and frankly the higher the bar to admissibility in the long run, the better for everyone. Most importantly for the general public because the right people will be caught and punished for crimes and the wrong people won't be. We will be able to solve crimes better. And there's just so much that can come from it. And so a lot of people on this PCAST have worked very hard on this project. Mike McQuade, Jim Gates who has been working on the commission, Bill Press, Susan Graham, Dan Schrag, Diana Pankevich has been staffing this effort. While we're not done and in a position to put up recommendations today, I did want to give this full report of the work in public session of the work that has gone on and the framing for it and throw it open to any discussion we might want to have at this meeting. I'll stop there.

>> JOHN HOLDREN: Questions, comments? Maxine.

>> MAXINE SAVITZ: That a very important report and you are doing well. You're focusing on the federal, which is appropriate. So many of these cases are at the state level and local level. If the guidelines are accepted at the federal level, how is that implemented at the state level?

>> ERIC LANDER: In the United States we have 51 jurisdictions to think about at least, and there are sub-jurisdictions under those. It happens in this case that the federal courts operate under the federal rules of evidence, particularly this thing I refer to as rule 702. About half the states have adopted the federal rules of evidence in its exact form or in some modified form. So while precedents in the federal courts don't automatically apply to criminal cases in the states, it seems likely to me that if they follow the federal rules broadly, the advice we're offering is applicable to those states. The other 25 or so states follow the older Fry standard after the case U.S. vs. Fry. It's different, but not so radically different that what we're saying can't be understood within the Fry context. We're not going to attempt to frame this for each of 51 different jurisdictions of course. But I think as framed, whether you're under federal rules of evidence of this earlier Fry standard, I think what we say should be usable by a judge in any of those settings. The question of whether a technology is foundationally valid is not case specific or law specific. No court really wants to admit a technology when no one has checked empirically whether it gets you the right answer. So that's really what will drive it. So even though we are staying in our lane by providing advice to the federal government, as we are a federal advisory committee, I believe that advice is going to be quite usable by states, as well.

>> JOHN HOLDREN: Jim Gates?

>> JAMES GATES: Thank you and thank you Eric for giving us this overview of this project I wanted to commend the working group and the group within PCAST who has been doing this, because I have been as Eric mentioned, I've used the analogy on Hadrian's Wall, I have for over a year been working on the forensics commission. One of the things I admire about the effort underway here is we have segmented the problem in a way that corresponds to what I've seen on the commission. There is indeed an issue to the foundational validity of the problem. That's one issue that one can see in the way that forensics is presently practiced. But there's a separate problem that you are very much aware of. When forensics experts get in the courtroom, the way in which they testify about the reliability of the results that are found in the laboratory are also itself problematical. Although our report doesn't deal directly with that issue, we do call it out. That's another area in which I think the community, the forensics community itself, under the gentle prodding shall we say of our effort will intend to correct matters. I want to say that I have a lot of confidence that we're moving properly in this.

>> JOHN HOLDREN: Thank you. Seeing no other flags up, thank you Eric for that summary.

Near Earth Objects

>>JOHN HOLDREN: We will now move to our Near Earth objects. If we could have the four panelists go to the front of the room and we'll get your name tags up there. The topics of near earth objects is one that I have long been interested in as has PCAST member Chris Chyba. It is one the President is interested in. His interest was particularly peaked early in the administration when two smallish Near Earth objects passed the earth inside the orbit of the moon. That gets your attention. It gets your attention even more when you look at the numbers of near earth objects on trajectories that might ultimately intersect that of the earth and what could happen if a big one hit. I sometimes say that our task is to prove that we're smarter than the dinosaurs, most of which appear to have gone extinct about 65 million years ago as a result of a very large asteroid impact in the Yucatan. I'm very pleased that had we have a terrific panel this morning. The panelists are Benjamin Alvin Drew, OSTP Assistant Director for Space and Aviation Security, Lindley Johnson, Program Executive for Near Earth Object Programs and Planetary Defense Officer in the Planetary Science Division of NASA Headquarters, the Science Mission Directorate, Bhavya Lal, Research Staff Member, Institute for Defense Analyses, Science and Technology Policy Institute, and Leviticus A. Lewis, Chief of the National Response Coordination Branch of the Federal Emergency Management Agency, FEMA. Their more detailed bios are in the possession of all of the PCAST members in your folders. I will not take the time of the panel to recite the members' many accomplishments. But let me thank you for being with us this morning. I'll turn it over to you. I imagine you have probably agreed on an order. So please take it away.

>> ALVIN DREW: Thank you Dr. Holdren. Good morning everyone. I'm Alvin Drew, and I'm the co-chair of this committee on detecting and mitigating the impact of Damion here along with Lindley Johnson, with the charter of trying to prevent us from meeting the same fate as the dinosaurs from large asteroids or being bedeviled in the meantime by a smaller ones along the way. The committee was set up initially with the idea of trying to deflect or trying to disperse things that were nearby. Couldn't quite pull it out complete from the problem of keeping custody of these things out there. Bhavya Lal will talk about is this really a problem. It's a very low probability event, but very high impact if it does

happen. Lindley Johnson will talk about his ongoing efforts to hunt for near earth objects. He has been doing that for decades now. And Leviticus A. Lewis will talk about FEMAs preparedness and post-strike response for near earth objects. Dr. Holdren talked about some objects that came close to the earth, back on Ash Wednesday of 2010, a 125 ton object entered the earth's atmosphere over the south Pacific. Left a big fiery trail of plasma over the top of the isthmus of Central America and finally came to earth's surface over Central Florida. Fortunately there were no casualties. The name of the object was the, I find it ironic right now I'm in part of the solution, when for a few brief fiery moments I was part of the problem. So the problem with trying to get rid of near-earth objects from hitting the earth, aside from the ones we intend to have come back to the earth is hard to deconflate from the task of detecting and dealing with the strike. They all come together. If I'm going to try to nudge an object away from hitting the earth or somehow disperse it, the first thing I need to know is the information I need to get is from the asteroid hunters out there. I need to characterize them, and to decide what to do about them. I need to know what would have happened if this were to strike the earth. And that comes from the folks at FEMA doing okay, this is something we really don't want to have hitting us, because the consequences are too onerous to bear or consider.

We have this whole continuous chain of getting rid of these asteroids and what we do from start to finish. We have the detection location characterization part, the warning part giving us the data so I can figure out what we can do about them and Lyndley will talk about that. The deflection and dispersal. The core of what we're working on in this working group. If that fails, what do we do here on Earth to prepare for that? And if something does hit the Earth, how do we go back and clean it up? Underpinning all of those things, no matter which phase we're talking about, are two basic things. One of those is the modeling and simulation tools. You're talking about things of very spare data sets out there, and very long distances from the earth. And it's hard to gather the data from them. You need some very intelligent guess work to deal with the large uncertainty bands around these things and where they're going to hit and what they're going to do. We need modeling and simulation tools a lot of science behind that. And anything that hits the earth is going to have global implications if it is a small thing, if it comes down and hits the earth, you want to be able to have good communication. So the international cooperation part is going to touch us, every one of these, no matter which side of this aspect of the problem you're talking about. So on mitigation, here are the things that keep me up at night. Answering the question what should and can be done and when do I need to know it by? There are some very different characteristics between a large object that is a long distance away from the earth and we have decades to respond to it. And one that is smaller and much closer in, like the one that surprised us back in February of 2013. We had no warning on that one. And very different things from that whole chain of custody, from the time we find it, to the time we have to go and do something about it. These parts NASA has a good handle on. The parts we need to work on and assess and figure out as part of this preparation. The table on the side talks about the warning time you have before impact. This one talks about the size of the asteroid and the scope of the effects. Look for that in Lindley's reports, and you'll see it again in his slides in greater detail. I'm concerned about this part that says provided we're ready to launch, anything that goes out into space. By my survey, we don't have anything ready to launch right now. So it looks more like this. Anything inside this side of 2026 increasingly becomes more of a civil defense issue no matter what the size of the asteroid is. So the charter here is what parts do we need to have ready for launch in time to make this a realistic chart than we had before so were are not increasingly panicked when something is coming closer to us. And with that, I'll hand you over to Bhavya Lal. Thank you.

>> BHAVYA LAL: Could you switch to my slide set? As Alvin said, I'll talk about what is the problem we are trying to solve her. I'll be quick so we can move onto the asteroid hunting and the cool parts. The asteroid threat didn't start with Hollywood making Armageddon or Deep Impact. The earth has been bombarded since it was formed billions of years ago. The common ones, examples we do talk about were 65 million years ago. Dr. Holdren made the comment that may have caused the extinction of not just dinosaurs, but 75% of all non-avian life on earth. There was a 10 kilometer wide near earth object. Just to make sure we don't think this is something that happens in pre-history, you know, when I was starting my first job, I remember watching pictures of a comet Shoemaker-Levy 9 that hit Jupiter. It had 21 pieces, some of them as large as two kilometers in diameter. It moved 60 kilometers a second. It hit Jupiter with the impact of the entire of arsenal of all of earth's weapons. This was the kind of hit that would take earth out essentially. Back on earth, 50 thousand years ago there was an impact of a near-earth object. We think it was about 45 meters wide. Because it was metallic and not stony, it hit the ground. Stony ones tend to be air bursts or just get destroyed in a fire ball in the atmosphere. Again, moving pretty fast. 20 kilometers a second. The blast equivalent was about 200 megatons of TNT equivalent. And it made a crater that was about a mile wide and 570 feet deep. So a small object 45 meters making a pretty big impact. More recently in 1908 in Tunguska, Russia a fast-moving NEO. This was most likely stony, fragmented at about 10 kilometers above the earth with a blast equivalent of five megatons of TNT, and it destroyed 2,000 square kilometers of forest. And just very recently in 2013, in Chelyabinsk Russia, there was an air burst of a very small sized neo as I talked about with the others, about 20 meters, but it had the equivalent of 30 Hiroshima bombs so again very powerful. It is a small city, Chelyabinsk, It injured about 1,600 people, caused about a billion rubles in property damage. So we have the very big, the ten kilometer sized asteroids. And then we have the tens of thousands of meteoroids that enter Earth's atmosphere every day that are dust size actually, more than tens of thousands. What is the right size to be worried about? I think that is an answer we don't know and Lindley is going to talk about it. Just to give you a sense, if there was a Tunguska coming over New York or San Francisco or Washington, D.C., this is going to be a pretty major impact. New York alone has over 8 million people. An air burst might have Tunguska, 2,000 square miles of trees that were flattened. We're talking about flattening a major US city. I don't want to find a silver lining here, but if we were to, this is a local issue. There is likely going to be no global challenges like kicking up enough dust that we have a nuclear winter type of situation with something this small. So thinking again about smaller NEOs, there's a lot of stuff going on in this chart. The X-axis is the equivalent of size. How big the neo would be and the Y-axis is the number. On the right side you see the kilometer and on there are a thousandish NEOs that are about that range. But if you start to look at the smaller Tunguska sizes, we are looking at a million asteroids that are that size. It's a substantial number. By extension, the more, the smaller entities tend to come more frequently, so again looking at the chart going from the bottom to the top for the very large objects, ten kilometers, there's about, we think there's about four of them. And they come every hundred million years or so. Not that it's not something to worry about, but potentially not to worry about in the very short term. Moving up as you come to the 50 meter asteroid, it comes about every 2,000 years, and again these numbers are approximate because there's only so much research we have. We actually don't know how many there are. Looking smaller sizes, we are looking at impact maybe every hundred years or so. And there's more than a million of those. And of course the important thing is we actually don't know where they are. Going back to the chart that I had before with a little bit more information on it, you see that the red line is essentially the numbers. Following the parallel. The blue line is how much of the survey has been complete. And Lindley will talk more about that. But the green bars are the important things to

see. You see up until about a kilometer our survey is pretty complete. We know where we have detected them and where they are. But as you start to go leftward, you see that our inventory is really incomplete. So I think obviously we need to worry about larger asteroids, which are the civilization enders, but we need to worry about the smaller ones, too. Not only because it can cause damage that could be substantial, but they just come more frequently. So in our lifetime we could see one of those. I think our saving grace is the population isn't everywhere. Most of earth is water and even when there's land there's different levels of population distribution. So we hope a small NEO will hit where there is no people. But hope is not a plan. To talk about that plan, I would like to turn it over to Lindley Johnson from NASA.

>> LINDLEY JOHNSON: Okay. Now that Bhavya has scared you half to death, I'm here to tell you what we are doing at NASA and with our partnerships across the U.S. government and internationally in this area. I head up what we have come to call the Planetary Defense Coordination office at NASA. This office was recently set up and formalized. But NASA as you'll see later in my briefing has been looking at this problem a number of years. But our office is set up to lead both national and international efforts first of all to detect any potential impact threat. You got to find them first. You can't do anything about them unless you can find them. And hopefully a number of years before they are impact threats. So we have a chance to do something about them. We also are involved in a lot of work to figure out exactly what is the threat and at what size object and what composition of objects? These asteroids of course come in different compositions as Bhavya alluded to. Whether they are metal rich or fluff balls of a lot of volatiles like comets. So those same-size objects with those different compositions could do different levels of damage. So some of our work is to assess four different size objects, what the threat level might be and really to establish at what range threshold are the objects large enough that we want to for sure find them in advance so we can do a space intercept. And below what size level could we take the hit? Particularly if we know if the object is headed to mid ocean or a largely unpopulated area. It's probably not worth the cost of undertaking a space mitigation campaign. If we know it's only a 30 or 40 meter size object that's going to hit in the middle of the Pacific, assuming it doesn't cause a large tsunami, and that is something else we are studying and these potential effects area to understand what an impact a tsunami might amount to. There's a lot of dichotomy right now in the modeling for impact-caused tsunamis, and we're working that out. And also developing strategies to be able to mitigate any impact effects both in space and here on earth. Working with my colleague here over on the left. So the defense coordination office is set up this way. First of all we have the near earth object observation program. This is a legacy program that NASA has been doing since '98. And we have a number of projects that are searching for these objects as well as taking data to characterize them so we understand what the population is out there and what it amounts to. Then down the middle here we have officers that are working. The interagency and emergency response working with FEMA and others as to first of all when we find an object that is an impact threat, getting the warning out to the right government agencies and others, and then working with FEMA in emergency response planning. That work goes on right now. And L.A. will tell you more about that. And making sure that we are prepared as much as we can be to respond should an impact threat be detected. And the third area we are working on mitigation research projects, trying to figure out if we are able to find them far enough ahead of time what we could do in space to deflect these objects off the course. Or if it's a more short-term warning, what could we do to break them up so that the impact on the earth would not be as bad. And perhaps earth's atmosphere can take care of what's left like it does every day for us with the small stuff we get hit every day with. The observation program started in '98 with an agreement with congress that we would find at least 90% of the one kilometer

and larger objects. We were able to reach that goal in 2010, having found some 850 to 870 of these objects in a population that is a little shy of a thousand. That in itself taught us something about the population. Going into this, we thought the population was probably about twice that much. But as we conducted the survey, we found that it was only about a thousand one kilometer and larger. But in the meantime, our objectives were moved as we began to realize that the objects a lot smaller than one kilometer in size could be a bad day for the area of the earth. And with the Authorization Act of 2005, Congress amended NASA's charter to make this work. One of the important activities that NASA should be involved in. And established our current objective of finding at least 90% of the 140 meter and larger objects within a 15-year period. This is a simplified version of the chart that Bhavya showed us. This is the statistical analysis of the known population shows us. That the entire population for the various sizes, this is work that is done by Al Harris who is a very prominent in the field of working the NEO population and understanding the population. We update our population model every two to three years. The latest update was done in 2004. And Bhavya showed you this chart. For the one kilometer and larger, we have done a good job finding most of that population. We feel we know of any objects that are 5-10 kilometers in size and larger. We know where all those are. The 1-5 kilometers, there are still a few out there to be found on the order of a few dozen. But our original objective has been accomplished. So now we're working on this objective of finding them all down to 140 meters or so in size. As you see with the population completeness curve in blue, as we drop below one kilometer in size, our understanding of the population drops off rapidly because the current assets that we use weren't designed to find asteroids in the first place, assets that we were using. We've adapted to it. But they certainly aren't highly capable of finding the smaller ones in a timely manner. These are our current search programs that are funded by NASA. But first I want to point out the two very important data analysis and processing nodes in our system. One is a minor planet center. They've been in existence for decades. Their job has been to catalog the smaller bodies in the solar system. Asteroids, comets, kiper belt objects. They do that for us. They are the International Astronomical Union sanctioned database. All the astronomers who do this type of work in the world know to send their data into the minor planet center. You can see all their data on their website. We also have established the Center for NEO Studies out at the jet propulsion laboratory. That is where the more precision type of determination is done. Once minor planet centers have established what the orbit of an object is, determining it is a near earth object for instance, then JPL takes over and does a more high-precision orbit determination with all the observation data that we have, and they're able to project confidently the orbits out to about a century to determine if an object is an impact hazard to the earth. Not only the earth, but also other planets and large bodies in the solar system. If there were going to be an impact on Mars, we would want to know about that. That would be a very interesting science experiment to see an impact on Mars. And that's all done through heavily automated system. It normally involves human interaction with it. When an object pops up that does show a high probability of impact. And they go in and make sure that we really understand what we're looking at. I should also point out that we do this in parallel with our colleagues in Europe. They have a similar system to JPL in predicting the hazard and the potential of impact. And we compare results of course before we would announce any particular impact. The three telescope systems you see along the bottom. These are some of the ones doing most of the work in discovering asteroids. Linear is a project that is operated by M.I.T. Lincoln Labs using the Air Force space surveillance assets. They were using the one meter ground based electrical deep earth surveillance system. For a number of years, prototype telescopes of that, but as the air force has moved to a new space telescope that has been developed by DARPA, MIT Lincoln Labs is working with us and the Air Force to install asteroid detection tracking capability on that telescope, as well. Right now, it operates in White Sands.

It's due to move to Australia in the future. University of Arizona operates three telescopes for us, collectively called the Catalina Sky Survey. And University of Hawaii operates the Pan Star system. A 1.8 meter telescope and a second 1.8 meter telescope just coming online this fall. We also adapted one space based asset. The wide field infrared survey explorer was an astrophysics mission developed to build up an infrared background of the sky for a James Web telescope. We quickly as we were developing it realized that with all the images it was taking of the infrared sky, we would find the asteroids in there, too. And so we adapted it with additional processing project called NEO wise, to do that during its prime mission in 2010. But as our program has gotten more funding in the last few years, we were able to bring that. It only had a one year mission with astrophysics and then it was put into hibernation. But as we got additional funding, we were able to bring it out of hibernation and put it in full-time use as an asteroid detection and tracking. So this chart shows you the discoveries each year of the near earth objects by these various projects. You see linear and its earlier version was one of the big discoveries through the early part of the program. It started in '98 and then Catalina Sky Survey became the prominent project. And now Pan Stars is now picking up a lot of the objects in the current endeavor. With pan-STARRS coming on full board, we've been able to increase our discovery rate per year up to about 1500 near earth objects we're breaking our record. And in 2016 we're breaking that record even with already 823 found in the first five months of this year. This is a cumulative total of NEOs, or near earth asteroids I should say since have been found at the start of the NEO program, in '98 there were only about 500 known near earth asteroids. But as our capabilities have increased, our discovery curve is going expediential there, as you can see. Total of all known near earth asteroids, a little over 14,000. We'll breakthrough 15,000 by the end of the year. Also there are 106 comets that are in orbits comets that come within 30 million miles of the earth, as well. Almost 1700 of them are in orbits that we consider hazardous. They come within 5 million miles of the earth's orbit. And over time they could wander into collision with the earth. Of the one kilometer and larger, we have 875 in our catalog, of which 157 are in the hazardous orbits. For the objective, 140 meter and larger, a little over 7,000 now in the catalog. About half of the population are larger. But that is an observational bias. The smaller objects are certainly a lot more of them than the 140 meter and larger. It's just that we've only been able to develop the capability to see the smaller ones further out in the later years. The earlier graph is a little deceptive. The small triangle looks smaller than the big one kilometer or larger triangle. So I break it down with a pie chart. 140 meter population. It is estimated to be between 25 and 26 thousand objects. The one kilometer and larger represents around 4% of that population of which we have found most of those. Three hundred meters to one kilometer in size, is about 30% of the population, and we have found about half of that population. But once we drop down in size below that, the larger part of the population 140 meters to 160 meters represents about 65-66%. And we have yet to find 60% of that overall population. So together, the two known areas, we still have about 75% of this population to find in our current objective. And we won't find them all by 2020. We use a number of assets also to characterize the objects. Once we find them, a more detailed observation of them. We use the two planetary radars that we have. The Goldstone is part of NASA's deep space network. And then the Arecibo observatory that is owned and operated by the NSF that NASA has the radar capability on. NASA has its own infrared telescope facility, ground-based three meter telescope on Monacaya that is used to determine the composition of these objects once we find them. And we also pressed into service the Spitzer space telescope when we can, where it has access to these objects to learn more about their sizes. So we contribute to the continued operations of Spitzer. Just a few words about international cooperation. In February of 2013, when Chelyabinsk happened, I and my colleagues from other nations were at a Committee for Peaceful Users of Outer Space science and technical subcommittee meeting about to brief our recommendations about the

international committee should do about near earth objects and lo and behold that's the morning that Chelyabinsk happened. That was mother nature putting in an exclamation point on our recommendation. What has been agreed to end that forum is that the member states should operate as part of an international asteroid warning network and pool our assets of observers, analysts, and modelers to find and detect and track and characterize the population to the best of our collective ability. And then also establish an international forum for the space agencies to be able to gather and talk about technologies and techniques that are needed for an in-space what we call the space mission mitigation planning or advisory group. So we're all working together to develop what the best response may be to a detected impact threat. And we do that all with the committee and with the support and sponsorship of the Office of Outerspace Affairs. International asteroid warning network in 2015. These are red dots that depict all of the observatories around the world that contributed observations to the planet center. Some 20 million observations from almost 40 countries. You saw this chart earlier. This comes out of the report from the National Research Council, a study that was done in 2009 and reported out in 2010 of what might we do to mitigate an object deflected that was on course for an impact? The leading three technologies, techniques that are thought to be most viable for doing this given our current technology is of course there's always the nuclear option, which we would prefer not to use. We would like to find them much further out. Then we could do something else. But if they are particularly large, that probably is our only recourse that would pack enough energy to do what would need to be done. But there are two other techniques, which would be effective against the larger part of the population, 100 meter or so in size. The first being the kinetic impacter. You just hit the object with spacecraft going fast enough that it would impart a change in velocity. And if you do this several years in advance, you only need to change the velocity of the object by a kilometer. I'm sorry. A centimeter or so per second so a few years down the line instead of it being impacted, it will be a complete miss of the earth. Then if you've got more time, this idea of a gravity tractor, which is very elegant in the fact that you don't have to even touch the object. You just use the laws of gravity to position the spacecraft off to the side station keep by the object and use gravity as a tug rope to pull it off onto another trajectory during a different course of time. This chart may be a little conservative on the area that the gravity tractor might be effective, but certainly if you've got 15-20 years and it's a small object, this is a viable technique and we are working to demonstrate these two techniques: Kinetic impacter and gravity tractor. Also working in a nuclear realm though, NASA works with the Department of Energy and the National Nuclear Security Administration in investigating the approaches that might have to be taken either within a short-term warning or with a large object. As far as a kinetic impacter technique, we are working with the European Space Agency on a concept called the Asteroid Impact Deflection Assessment. We are currently in formulation phase A studies where the European space agency will launch the asteroid impact monitor, that is the spacecraft to go out and rendezvous with the potential target and understand its composition and provide more detailed data on the object than we can get from the ground. And then the U.S. NASA would come along with the DART, the double asteroid redirect test. And the reason it's called the double asteroid redirect test is because the selected target for demonstration of this target is the asteroid Didymos, which is a binary near-earth asteroid. We would hit the moon of Didymos, affectionately called Didy moon. That's not the real name for it. But the reason we want to demonstrate this on the moon is it's about 140 meters in size that we are searching for. We want to make sure that we can hit a target that is that small millions of miles in space. And it's also easy to see the effects of the deflection and the period from ground based telescopes. The effects of the deflection and the period of the moon would be affected. And that's an easy thing to see even from ground-based telescopes. This would be an important demonstration of the kinetic impact

deflection. The other nice thing about it is it's an international collaborative effort, not only with the Europeans, but the Japanese are also interested in participating in this mission. And then the other large project that we were working with, coordination as part of our office, coordinating with the asteroid redirect mission, which is a leading program for NASA to demonstrate the technologies and techniques that are needed on our journey to Mars, being able the move large masses and cargo from the earth to Mars to support the human exploration of Mars. The near earth object program provides the identify segment of this mission using technologies and capabilities that we have to detect and characterize near earth objects. So we have a few candidates for this mission already. But we continue to search for even better candidates. We still have a few years before the decision would have to be made as to what the target would be. The asteroid robotic redirect mission is depicted here in the middle where the robotic spacecraft with the solar electric propulsion technology and the grappling technology that is being developed would go to a near earth asteroid, collect a large tens of tons boulder off the surface and grasp that in its arms and bring it back to suslunar space where the human group would go up and explore and collect samples and practice docking in deep space docking and rendezvous and EVA techniques. As far as a robotic spacecraft, we are particularly interested in it from the planetary defense aspect. Going to this near earth asteroid, collecting its mass off it, because before it comes back to the moon, we want to do a defense planetary defense demo of the gravity technique with this mass. Station keeping off to the side of the asteroid to slowly pull it off of its trajectory to demonstrate that technique really does work, and how effective it can be. And so with that, I'm going to turn it over to L.A.

>> L.A. Lewis: Thank you for inviting me here. I never thought I would be here with NASA and two rocket scientist being a FEMA guy. Again, I'm L.A. Lewis, and I'm from FEMA. I've been working with Lindley since 2010 with the letter that was sent to Congress, I wanted to talk about what the responsibilities were. The initial task was to come up with a warning mechanism should this event happen. And Lindley and I working together, FEMA already has an in-place national warning system that we have used for other emergencies, and we're going to probably work on modifying that existing framework for this scenario. So we formed the Planetary Impact Emergency Response Working group back in 2013. It's a joint effort sponsored by the FEMA Response Directorate and the Planetary Science Division at NASA. Our mission is to provide a forum for developing essential recommendations for our senior leadership so they can make informed decision to respond to what we consider to be a very unique type of emergency. Everybody is used to hurricanes, tornadoes, earthquakes, et cetera. And a near earth object impact hasn't been witnessed by anyone of a large size since Tunguska I guess, and Chelyabinsk was a good wakeup call. In fact I got a lot of phone calls from my colleagues wondering why we were not warned about this type of object so that got a lot of interest there. So that's what the PIERWG does. Our role is to extend working on what will we tell the emergency managers in the United States? How do we send this information to the public? What do we tell them to prepare for? How do we give emergency managers that right information so that they can respond to this in their localities, in their states? Again, everybody is used to seeing a hurricane cone on the news. Nobody will be used to seeing Monte Carlo points on a map with asteroid impacts. We need to be able to explain that and also be sure that we are considered the primary source of knowledge, as you can imagine. Once this gets out, there won't be a secret that this is going to be an impact. The experts will be on the news, and we'll be competing with them to make sure we get the right information. This is going to be analogous to re-entering large space debris to hurricane warning procedures. We know how to do that. We have procedures in place whenever we have reentries of large satellites. The I-SATs and other things that have come back to earth. TRIM a couple of years ago. We went through a

whole procedure on that. The emergency community is used to that. We're going to use that as a basis for moving forward. And the other unique challenge to this as we had our PIERWG meeting a few weeks ago, the timelines for decisions. If you have hours or days or weeks, it's one way you have to alert to public. But if you have years or tens of years, how you do that to the public and prepare emergency management is another story. People are not going to want to pay attention. And the scenario that we practiced on our table top exercises is Americans will first get excited about it when we first announce it. And if you say it's going to be ten years, no one will pay attention to it, but then T minus six months everyone will ask what should we be doing. Of course, what is explained is that NASA is the lead in this. We'll be depending on them for the scientific information and the information on where it's probably going to impact. And also the efforts that they're making in modeling. Because one of the things we wanted to do also in informing emergency managers and leadership in response is why is it makes a difference to know what the asteroid is made of? Whether it's a stony body or iron, nickel, or metallic, how large it is, and how fast it is. That all makes a difference. The impact on the ground, how much damage there's going to be, and that helps us in our preparation efforts. Again, the PIERWG goal is to gather all of this information, and we act as a clearinghouse for our senior leadership, particularly the emergency management community, and translate all of the science and modeling data into real actionable things for the emergency management agencies to do. How long do they have? It's just different from any other response that we have to make. One of the other things, Lindley mentioned tsunamis. We know about earthquake-based tsunamis, we assume tsunamis will be the same. But if it is an impact tsunami, will it be the same. But we don't know that. We're still working on it. Will the effects when it hits land be different Will it be depending how it is if it's far off in the ocean it is or how far out on the continental shelf? Is it different if it lands on the east coast or the west coast in the ocean? Those are the things that we need to know. The membership, we have two groups that we work with interagency at FEMA. The emergency support function leadership group. There are 15 emergency support functions, there are 12 recovery support functions. There are two different parts of the emergency support functions are the guys who are going to help respond, who help aid the Federal coordination. Recovery is what's afterward. So say we have a large impactor and it's going to impact a significant part of U.S. infrastructure, a major U.S. city. What are going to be the long-term goals for recovering from that? And will that be different from a devastating earthquake, depending on the size of the impact? We want to be able to provide those kinds of groups, the specific information that is unique to an asteroid impact. I won't read all of this. This just gives more of the details. You can read it at your leisure. Just kind of tell you that the PIERWG is going to try to coordinate all the different activities that can happen, the main thing is what is different from an asteroid impact as opposed to an earthquake or hurricane or another emergency. And this is not to say that we're spending nights staying awake at this. This is another emergency on the list of emergencies that we have to respond to. Because of the unique nature, we're starting our partnership with NASA to make sure we understand this phenomenon and understand the science behind it and why the science is different from the other emergencies that we're familiar with and make sure that we relay that to our senior leadership. We're going to have teams. Right now we have two teams. With the composition of the PIERWG we'll divide it up into teams where we have specific things. The project that we're working on now is trying to narrow down what does the alert message out to the public say depending on this scenario. Whether we have days, hours, or we also understand there is the possibility of no-notice impact. And then we'll handle it like our other emergencies. We're not planning on developing a specific plan for asteroids at this time. But we have federal interagency operational plans that address the various types of emergencies. So depending on the information gathered in this effort emergency, we'll be using those already-determined responses to kind of model

what we'll need in particular for an asteroid impact. Next steps. We're going to work on again the information for warning. Make sure we are tied into what the international asteroid warning network is going to do, and we're going to probably use variations of our current satellite reentry message format. But depending on how the research is going, we may have to modify that somewhat. And our next big thing right now is planning for our third table top exercise. Going to try to take a slightly different approach this time. We have done two table tops in Washington, D.C. We like to think of getting out of Washington, D.C. to get a different flavor. And the next table top invite the city we've chosen for our destruction, invite their emergency managers and the state emergency managers and actually work through the exercise with them. And then that way we'll get a different flavor from just having the Washington experts and thinking we have a good idea what they're going to ask. But it would be good to see if we have some local officials in the next exercise and to get their reaction to this event. And that's essentially our part. We hopefully won't be needing the services. Our colleagues here will be successful and they won't be needing us. Thank you.

>> JOHN HOLDREN: Good. We have time for a few questions. And there are probably more flags up than we might really have time for. So I urge everybody to be concise. Chris Chyba is first.

>>CHRISTOPHER CHYBA: Thanks John, and thanks for a fascinating set of presentations. I can't tell you how pleased I am to hear that all this planning is going on. It's really good news. As you well know, having decades of warning time would make a tremendous difference across the board. Huge advantages including the opportunity to try more than once if we don't quite do it right the first time. So my question comes in two parts. I'm sorry John. My first question is given that I would the almost overwhelming importance of having warning time, what is in fact now your estimate given the ongoing searches for objects larger than 140 meters? What is your estimate for when you'll have a catalog that is say more 90% complete? And in the event that we do have an object that is going to hit us some decades down the road, not only do we have to deflect it, but I'm curious what your thinking is of what kind of dialogue takes place within the international community of how it's going to be deflected and who is going to do it, and who has responsibility for making that decision?

>>LINDLEY JOHNSON: Well, with the pace of the current assets that we have searching, as I said we're finding, hopefully this year we'll be up to about 600 of the 140 meter and larger objects. But we have about 18,000 left to find. You can do the math there. It's about 30 years at the current pace. We do have plans for additional and more capable assets coming online. For instance we are working with the National Science Foundation and a large synoptic survey telescope when it comes online, working with them to develop the right techniques for using the vast amount of imaging that they're going to be taking to detect and track asteroids in that large data set. But the really most capable way of finding these objects would be to be able to do it in the I.R. and to do that, you've got to get above the earth's atmosphere. And so a space-based I.R. spacecraft that is specifically designed to detect and track asteroids would be the way we would like to be able to go if we had the resources to do that. To your other question, and working with the international community, that's what Same Page is all about. It is to try to put at least a template into place with the international community of how we would work together from the warning that we have an impact to putting an international campaign together to go do something about it, deflect it, disrupt it, depending on what kind of time we have available and what technology we have to do that. It's not just the technical side of it. But we're also looking at, you know, the political issues and the international legal issues, as well. In doing this as a part of that forum.

>> JOHN HOLDREN: Jim Gates is next.

>> JAMES GATES: Thank you, John. And thank you to the panel for that excellent briefing. My question has to do mostly with L.A.'s presentation at the end. You talked about the planning for disaster, preparedness of the nature that a tornado. I'm sorry. A hurricane or reentering space vehicle. But I'm a little bit worried about that. Because you see, I can imagine a scenario where if we have sufficient warning, non-experts get into the discussion outside of the government. And in particular, I'm wondering about what is your thoughts about external media validators who then reinforce your message and get the proper information out. Because in this age of loss of authority because of the internet, there are going to be a lot of people out there putting out a lot of misinformation. And I would like to hear something in your thinking about how to deal with that. The idea of a civilization extinctor. You can imagine someone saying gee, this is the end. But it may not be the end. What are you doing to deal with that problem?

>> L.A. Lewis: Thank you, sir. That's a good question. And both of our table tops previously, we discussed this possibility. It took up quite a bit of time. We talked about it at the last two planetary defense conferences. We were talking about the idea that because of the availability of this information on the internet, that unlike the movies, there is no way they're going to build a spaceship and orbit it for a year and nobody sees it. We give ourselves about 30 minutes before it's out that somebody knows there is going to be an impact and it is all over. We have actively discussed how do you counter all the new experts that will show up on CNN and Fox and MSNBC. So what we're thinking is when we have the meetings with the international asteroid warning network, we've got to involve the media, but we also have to make sure that we're as up front as possible with the public to make sure we get out in front early to show that this is the authoritative information and not making it so dire that people think there are no options. We're also talking about what we should do and whether we should have a website set up that people can go to and look at the data themselves, have people working with our public affairs, our external affairs personnel, and explaining the phenomenon to people right away, explaining what asteroids are, where they come from. Trying to get out as much information up front as soon as possible. But we recognize, sir, that there will be competition from the other experts. I know my other panelist have thought about that.

>> JAMES GATES: What about religious leaders? This will become such an issue.

>>ALVIN DREW: The other part is that we can bring down some of the uncertainty bands around the data. One of my fellow astronauts and asteroid hunters Ed Lu, he wants to exercise a near miss to see what the effect the uncertainty would have on property and property insurance values if something came by. Anything under the footprint would become uniquely un-insurable for a brief period of time, what that does to markets. The best we can do, we can't do anything about the culture part, we can get those numbers as tight as we can, and say yes we know we can be close, and yes we're going to miss. And this is the circle that is going to be hit. The more uncertainty we can knock off of it, the less speculation you leave out there for the Johnny come latelies.

>>JOHN HOLDREN: Susan Graham?

>> SUSAN GRAHAM: I too, want to thank you for these presentations, which are very interesting. I would like to know more about the international aspects of these activities. You touched on some of it in response to Chris. But it would seem that the first stage you described, developing the inventory of objects, the detection and so on would be an issue in which there is international interest. There is no reason why it affects us more than it affects any other country. And yet your description was mostly about what we're doing to do this detection which gets increasingly expensive as we get to the harder things to detect. So what's going on internationally to share this responsibility as well as sharing the information?

>> LINDLEY JOHNSON: Well it is true that the U.S. does have the largest effort here. The U.S. systems are finding over 95% of the objects every year and we have the most capable systems. But that was part of the idea about establishing the International Asteroid Warning Network. With the endorsement of the United Nations so that other countries first of all can learn about what is being done, and how they might contribute. One of the things, in fact just this year at the committee meeting, we had an open forum with the international community describing to them about how we do what we do and how observatories around the world could join the effort and become part of the network. How to send their observations into the minor planet center and those kinds of things. So one is informing them about how they can participate and then continuing to encourage them to join in the effort.

>> BHAVYA LAL: If I could also add, I think we did talk more about the U.S. efforts, but it is an international community. The last planetary defense conference was in Italy. And it was very European heavy. There is international interest. There was Asian participation. Maybe not a lot from China and India. But the next one is in Tokyo. I think that now at the moment, most of the detection efforts are mostly U.S. centric. But on the mitigation piece, there is more effort. ISA has some efforts, so there is European and Asian programs on the topic.

>> LINDLEY JOHNSON: They actually came to us with this idea of the asteroid impact deflection assessment mission. That is a largely European-initiated mission. And we are becoming a part of it. If they intend to go forward with their spacecraft, our intent is to go forward with ours.

>>JOHN HOLDREN: Bill Press?

>>WILLIAM PRESS: So I guess my question will sound a little bit like a joke, but I don't mean it that way. My question is about the lawyers. What is the legal framework? Can the President as Commander in Chief order an asteroid to be deflected? Does it take congressional action or international action? What is the relevant body of law on this?

>> LINDLEY JOHNSON: That is one of the issues and areas that Same Page is dealing with. One of the sub-working groups of Same Page is a legal group which we were establishing this year. Same Page has been going for a little over a year now. There are a number of legal issues with this. The space legal community has discussed and talked about this for a number of years. But not under a discipline forum I would say. So we're trying to do that under the Same Page.

>>ALVIN DREW: Of the existing laws, one of them prohibits nuclear weapons in space, so one is a nuclear warhead, not a weapon. Another part of these is extracting resources for our own use. I

jokingly note that one of the ways to get rid of our bigger asteroids is to declare it open to exploitation get it out there and have people out there mine it into extinction. But there are laws about that. And what you bring back and declare sovereign.

>> LINDLEY JOHNSON: One of the questions is if the United States or the United States and the Europeans attempt a deflection mission and it doesn't quite succeed and we move an asteroid that was going to impact in the middle of the Pacific to where it is going to impact in southeast Asia, who is responsible?

>>WILLIAM PRESS: Or on a smaller scale, if you break it into small pieces, and one of those pieces hits me, who do I sue?

(Laughter).

>> ALVIN DREW: Unless it's a very small piece.

>>JOHN HOLDREN: I'm going to have the last question here because we have pretty much exhausted the time. I have both one comment and one question. The comment is I think all of us in the science and engineering community need to get better at communicating the nature of stochastic processes. When you tell somebody that the mean return time for an asteroid of this size is a million years most members of the public think this is only a long-term issue. We don't have to worry about it in the short-term because it's going to be a million years until it happens. I think all of us know in this room probably know that an annual probability of one in a million doesn't mean you can safely wait a million years. It could happen tomorrow. It could happen if five years or ten. These probabilities are mean return times, not predictions of how long it's going to take to come back. This is a big problem. Because it has led people, I believe including the folks controlling the purse strings to underrate the importance of dealing with these very low probability, but extremely high impact possibilities. If you sort of think carefully about the value of our big cities or the value of our civilization, we are probably under-investing both in detection and in the development of technologies to deflect. That is just an observation of how we tell the story. My question has to do with the list of possible approaches to deflection, which listed only three. Kinetic impact, gravity tractor, and nuclear. And I'm just wondering. I have not actually gone back and read the academy report. But it strikes me that there is at least in principle another possibility, which is to use instead of a gravity tractor, use a thrust push. In other words, bring to the asteroid a thruster of some kind that could exert a thrust over a period of time. Obviously given the cost of transporting stuff into space, probably a chemical rocket would not be very attractive as a thruster. But I can imagine a solar ion thruster for example might be interesting. Has that been ruled out on the basis of detailed calculations that indicate it is just not as attractive as a gravity tractor?

>> LINDLEY JOHNSON: With the NRC report, those three techniques were determined to be the most viable at this time given our technology. The difficulty with a thruster, the complexity of trying to thrust is that these objects, particularly the smallest ones are spinning quite rapidly. And so you've got to have, if you're going to land on the object and try to thrust against it, you've got to have some way of compensating for that. Either, you know, a pulsing of the thrust at the right moment, which decreases the effectiveness of it considerably, or you have to de-spin this tens of tons mass, which may sound simple. But when you look at the numbers, it's quite complex. I wouldn't rule that out, but it is

considered add more complex approach than the three that we talked about.

>> JOHN HOLDREN: Okay, let me close this session.

>> BHAVYA LAL: Can I add one thing? The OSTP-lead working group that has been set up to address this challenge, DAMIAN, has five components. Detection, deflection, disruption, mitigation, recovery, and response. As far as developing the strategy and action plan for near -earth objects, one of the gap areas is likely the issue that you have which is are there other solutions that need to be looked at, that need to be developed. And you know, there's many suggestions in the community. One elegant one is painting the asteroid and using the thermal gradients to move it. All of those will get looked at, as well.

>> JOHN HOLDREN: Great. Thanks to the whole panel for a very informative set of presentations and good Q&A. We will now break for 15 minutes, and while we are a little bit behind schedule, that is not such a serious problem because I understand we only have one public comments, one public comment, and abundant time set aside for that. Let us return in 15 minutes.

>> Thank you for your continued interest.

[Applause]

Cryptocurrencies

>> JOHN HOLDREN: So Bill Press is going to moderate this next session, starting with the introduction of the panel. Bill, as most people in the room know is one of our two PCAST vice chairs, and is much more knowledgeable than I am certainly. I'll let the others speak for themselves on this particular topic. Bill?

>> BILL PRESS: Thank you John. After coming close to destroying the world in the previous session, I don't know what can be more upbeat than the idea that we can make money out of pure bits. Just money from nowhere. This session is on crypto currencies, which is in the popular imagination usually goes by the name Bitcoin, but I think as we're going to see there is a much more general and fundamental idea here, something that has the possibility of not only revolutionizing not only something having to do with money and finance, but a broader set of functions in our civilization as long as it's not destroyed by the asteroid.

We have four very distinguished speakers. And let me just introduce them by their titles. PCAST members, you have their full bios in front of you. They're going to speak not in the order that they're seated, but in this order. Joseph Bonneau is a postdoctoral researcher at Stanford and a technology fellow with the Electronic Frontier Foundation. Jerry Brito is Executive Director of the Coin Center, a not for profit study center. Simon Johnson is Ronald A Kurtz Professor of Entrepreneurship at the MIT Sloan School of Management. And Tim Grant is managing director of R3CEV, which I'll wait for him to speak to tell you what that is. Each speaker will maybe speak for 7-8 minutes maximum, and that will allow us a lot of time for conversation that we want to have with you.
So Joe, please take it off?

>> JOSEPH BONNEAU: Okay. Yeah, thanks for the intro. It's great to be here. So I guess just quickly by way of background. I'm an academic researcher. I've been looking at Bitcoin for about the past five years. From the point in time when you wanted to find out anything about Bitcoin, you really had to start digging into IRC channels and mailing list archives and weird places on the internet and look at source code. Now I can say on the academic side excitingly we have developed course materials. We have a Corcyra course that I worked on with Ed Felton. I worked with my colleagues at Princeton. We have a textbook coming out. There's a whole literature. A whole academic literature and research papers on Bitcoins. In the last five years, it's amazing how it has gone from such an obscure field of knowledge to we have some good technical resources out there. Lots and lots of people. I taught a course at Stanford this year, and we had undergrad 150 students show up to learn about crypto currencies. It's a really exciting topic within computer science. The good news is that we are gaining much more fundamental understanding. This is really sort of a technology that came from way outside of academia. Obviously on the personal level of the story of how Bitcoin got created. It's fascinating by this anonymous technologist. We don't really know who made it et cetera. But it came with no proofs, no definitions. It wasn't a very carefully thought through computer science system at the time it was launched. We had to develop a theory after the fact. That's the good news. We made a lot of progress. Our technical understanding of what crypto currencies are has expanded a lot. And I'll say kind of the other side of the coin there, we still don't really have good definitions of these things, and the terms get thrown around a lot in the popular discourse and people use them to mean very different things. So I'll just try and give a quick technical definition of some terminology, because I'm sure that we'll hear the terms crypto currency and block chain a lot today. When people talk about the whole space, those are the two overview terms that they use. And we don't have a universally agreed upon definition of what those things are. They're closer on the spectrum of buzzword and technical definition, they're still closer to buzz word. We would like to wrangle them to something we have a technical definition for. The definition I would give for crypto currency is it's a digital currency. Digital currency means it's represented in bits. There isn't a paper artifact or anything else that represents who owns the value. A crypto currency changes hands through the use of some cryptographic algorithm. Most of the time you do a digital signature, to say you want to send value from one person to another. There are other ways to send the information cryptographically. But usually we mean there's some digital artifact that has value. You compute a digital signature to send from one person to another. So note there are a lot of other digital currencies that aren't crypto currencies. Everything from gold in the World of Warcraft game. You could argue the way that we use credit cards most of the time, they're essentially digital currencies, because we're not interacting with the physical artifact as much. So that is really the power there is that we can use cryptography directly to transfer money to send from one party to another and you can do it in a permissionless way. If you can compute the cryptographic algorithm, then you are able to send the money. It sounds like a very small step. Who cares about that fact? But when you, we've kind of realized slowly that that's really, really powerful. That means as a result of some cryptographic protocol, you can automatically transfer money. It gives you this whole new toolbox when we are designing online protocols everything from designing an auction online to two people playing chess online, you can have the results of that interaction actually move value between the two parties. And you can do it automatically without having to rely on some third party. Cryptocurrency, to me what's really power is we're using cryptography directly to transfer money between two parties. Another thing that we will talk about I am assuming are block chains. On one level a block chain is just a data structure where we have an append-only log, an ever growing log of data, we can keep adding to it. A cryptographic hash function is used so we constantly have a snapshot that captures the entire history of the system. But it's funny to call it a block chain because

that idea dates back at least to the early1990s. It wasn't called a block chain when it was first proposed, but the earliest cryptography papers that proposed this are at least 25 years old now. They weren't proposed in terms of the concept of money, they were proposed for maintaining a ledgers for historical archiving purposes like that. I think what goes from the pure data structure to something that we would call a block chain is there are precise rules about what kind of data that you would add. The technical term you could sometimes use would be a replicated state machine, which means you have some state of the system and there are specific rules for how that state can change to another state that everybody can verify. So it's replicated and everybody is running an algorithm that checks for valid state transitions, and can check that the block chain is only having data added to it according to the rules of some state machine. Bitcoin rules are fairly simple. There are basic sanity properties that you would want in a currency that you can't create or destroy value, and transactions have to actually be signed. People have proposed much more powerful versions of this block chain. Since then, it started with a few years of people saying it would be great if we had a little bit of functionality in these state machines that we could represent more complicated things. Famously people came up with Name Coin, because what if we could do a distributed naming system on top of this block chain. And now we have gotten to the point that with a theory of other proposals, where the state machine is essentially programmable. People can take any program, technically we say the system is turning complete. So any program that computer scientists know how to write down, you can represent in the rules of the state machine. And everybody can check that the states are being represented. So that represents, you know, in some sense the end game of power. We now have this block chain that can represent sort of arbitrarily complicated transactions and protocols between different parties, although we're still really just scratching the surface of how to program that and how to do useful things with that. So on the academic side, that's where a lot of the excitement is now, figuring out more complicated protocols besides just payment we can build using a more powerful block chain like a theorem. So I just wanted to kick off by saying just those notes on terminology. I'm sure a lot more questions will come up. But at a technical level, that's what I see as the big steps forward that we made in our thinking about this space. And I guess I'll turn it over to Jerry with that.

>> JERRY BRITO: So as Bill mentioned, I'm Jerry Brito. I'm the Executive Director of Coin Center. Coin Center is an independent nonprofit based here in Washington, D.C. We're focused on the public policy issues facing crypto currencies like Bitcoin and distributed decentralized computing platforms like Etherian. Given that vantage point I'm going to give you a high level overview of what are the regulatory questions and what is the regulatory landscapes surrounding these technologies. So the first question we have to ask ourselves is. Why are governments interested? We've seen a lot of activity where policymakers and regulators are interested in these. It's for a couple of reasons. First, the currency, the token that Joseph was describing, for the first time these technologies have allowed us to have provable scarcity online. These tokens can be limited in a certain way where you can show provably that when I transfer one to you in a peer to peer fashion, that is a token that you're getting. And this means that the token can represent anything. To date, these tokens have tended to represent money. So one Bitcoin today is worth about $440. That is an obvious application of a token that can be transferred in a peer to peer fashion. These tokens can represent anything. It can represent a particular house, a particular car, an ounce of gold, a share of stock. And again, they can be traded in a peer to peer fashion. And so as a result, financial applications that are build using crypto currency networks potentially implicate consumer protection, tax, securities and other regulations. And so these are all and have drawn the attention of policymakers. Crypto currencies as Joseph said are also open permissionless networks, a lot like the internet, and they're also decentralized, which means that

they lack intermediaries, and thus they're censorship resistant. What I mean is this, previous to the invention of Bitcoin, the first crypto currency, if somebody wanted to design or develop a financial application or an application that used a scarce token, they would have to get the permission of a third-party intermediary like PayPal or Bank of America typically through and API to build that application. Today because these networks are open and permissionless, they can develop by building the application and launching it on a network much like somebody could do Mark Zuckerberg could launch Facebook from his dorm room. This permissionlessness and resistance are the exact ingredients that allow for innovation to flourish through experimentation and they allow for innovative peer to peer uses like micro transactions like they weren't possible before. These same features have also attracted illicit users. And so crypto currencies have become the payment rails for online drug markets, and ransom ware. And as a result there's a lot of scrutiny from law enforcement agencies. Those are the two main areas where we see interest from government. The thing to notice here is we saw similar policy challenges emerge along with the original permissionless network of the internet. There were questions about consumer protections, tax, intellectual policy, and issues related to illicit uses, et cetera. But the framework for global electronic commerce, which laid out the Clinton administration's policy for the internet in July of 1997, it said that governments should recognize the unique qualities of the internet. And it went onto say that the genius and explosive success to the internet can be attributed in part to its decentralized nature and to its tradition of bottom-up governance. Accordingly, the regulatory framework established over the past 60 years for telecommunication, radio, and television may not fit the internet. Existing laws and regulations that may hinder electronic commerce should be reviewed and revised and eliminated to reflect the needs of the new electronic age. We're lucky that that forward-thinking policy was put in place, and today this same approach is advisable for crypto currencies. And luckily to date the U.S. government has grasped the potential of this technology. Big attention to crypto currencies really began in fall of 2013 with the first congressional hearings on crypto currencies. These were two paired Senate hearings. And industry, academia, government all participated in these, and the outcome was very positive. There was an understanding that this technology could really revolutionize finance, but anything that uses a ledger, which is anything that uses a database, which is just about anything. And the great thing about the outcome of these hearings is there you had the regulators on point at the moment, especially the Treasury Department and this is quote there are many legitimate uses of these technologies and the virtual currencies are absolutely legal. And they're very innovative and important for the economy. So that was sort of an overhang. It began in 2009. There was always a question of you're creating money out of thin air, is this legal? That was sort of put to rest here with these hearings in 2013. But what remained were a lot of policy details. And there are two major areas of regulatory activity that we've seen today. That has to do with consumer protection on one hand and on the other hand financial surveillance. I'll talk first about consumer protection. In 2014 you had the implosion of the largest Bitcoin exchange that was called Mt. Gox. And as a result, you had the loss of about 600 million dollars in assets by consumers. And this was the function of because Bitcoin was so new, it was something that really was sort of being developed by enthusiasts, by computer scientists who were having to go to those forums and crazy Reddit post to find out how to build it. There was no good way of buying and selling it to each other. And this one count called Mt. Gox sort of emerged as the one exchange. The exchange was seemingly built by amateurs and as a result it collapsed. This brought a lot of attention of what are the regulatory standards here. What we have seen since then is today you have at least half a dozen, if not more seriously regulated Bitcoin exchanges that are licensed and they are backed by serious investors and have professional management. And part of this is because of the licensing regime that has been put in place. Typically if you're not a bank, but you're

taking custody of consumer funds, you're going to be subject to state licensing, state money transmission licensing and today you have about a dozen states that are actively either developing new legislation to create new licenses for digital currencies, or they're amending their existing transmission licenses to accommodate these. New York was famously the first state to create the Bit-license for companies that are taking license of consumer funds but you have other states like Texas and Kansas who have applied their existing money transition licensing to the companies that operate in this space. And what's important to understand about the licensing here and the reason we have it and how we apply it is that the risk is presented when you have a company that takes custody of consumer funds, whether that's dollars or whether that is Bitcoin. And if you are holding onto somebody's Bitcoin, essentially holding onto their cryptographic keys you are being put in a position of trust and you need to be licensed. And licensing requires background checks, requires that you post a bond, requires that you get permission before you develop new products, etc. Now there are some issues with this, which is the following, that we used to be sort of cognizant about. Financial services that could previously only be offered through a full custodial service can now be offered without taking custody of consumer funds, and thereby posing little or no risk to consumers. Let me give you two simple examples. One would be Wallet Software. If I wanted to have Bitcoins, one was I could do it was have a relationship with a Bitcoin wallet company. I give them my Bitcoin and hold it for me, and I ask them to transact on my behalf the way I would do with Paypal. It's a traditional model and also licensed. But there's also the possibility where I could download software created by a company and I can have full custody of the Bitcoin myself on my computer, even if that software is being delivered through a browser, and even when looking at it, it looks very similar to a custodial service. Those kinds of services really increase consumer privacy, increase consumer protection because there is no company that can run away with the money. And as a result, they reduce risk. And so we should make sure that licensing is appropriately avoided there. Money transmission licensing can also present a barrier to innovation. Because number one, you need to get 50 licenses before you can operate. You have to get a license in each and every state in which you operate. And to date, these licenses are not forthcoming or they've been inconsistent, and it also potentially cancels out the advantages of having an open-permissionless platform. This is in contrast with other countries.

The E.U. has easy passporting of licenses. If you get a license in the U.K., you are good to go in every other state in the European Union. So that essentially is consumer protection. We license actors who are taking custody of funds, and hopefully we exclude from any licensing requirements those companies that are building out solutions that do not take custody of funds. The next big area is financial surveillance. And one important thing I need to note off the bat here is a crypto currency like Bitcoin is not anonymous, despite what many people read in the newspapers. It's better to call it pseudomonas. There is a record kept of every single transaction that is carried out over the network. To give you an example of a truly anonymous transaction would be a cash transaction. If I'm selling a bicycle at the flea market and Joseph comes along and he gives me a hundred dollar bill and I give him the bike, we part our separate ways. He doesn't know my name, I don't know his name. There is no record of that transaction- the date, the amount, the time, the purpose. That is a completely anonymous transaction. On the other hand you have something like say a credit card transaction, which is a perfectly identified transaction. If Joe were to pay me with a credit card, his bank knows his information, my bank knows my information, and there's a record kept of the date, time, and amount of that transaction. With the Bitcoin block chain, it’s a little bit of both - it's pseudomonas. There is a record kept of the date, time and amount - it's necessary. But our names are not necessarily tied to those transactions, certainly not on the public block chain. This presents sort of a dilemma for law enforcement who are used to being able to have somebody's name that they're investigating, being

able to go to a financial institution and saying can you show me all of Joe's financial records, and everybody who he has transacted with for a subpoena or search warrant. That is not possible on the Bitcoin network, in the sense that you don't know just looking at Joe's name, you don't know what transactions are there. It's a bit reversed. With Bitcoin you can see a transaction has happened, but you don't know who is attached to this transaction. You can then go to a financial intermediary, something like an exchange and say can you reveal to me who is the name? Who is the person associated with this Bitcoin transaction, and they can do that. It's sort of the inverse of what law enforcement has traditionally been used to, but still there are tools for them to investigate. So in order for them to have access to this information, they need to intermediaries, like exchanges, need to be required to record information about their customers. So in March of 2013 the Financial Crimes Enforcement Network, which is part of the Treasury Department issues guidance saying the crypto currencies exchanges are subject to the bank secrecy act. And so that means they must register...

>> BILL PRESS: Can you wind up in maybe a minute or two?

>> JERRY BRITO: Sorry. I'm taking a long time. And create records that they can then make available to law enforcement. So today law enforcement is able to complete their investigations. I'll stop there. I'll also say tax questions have come up, but they've been addressed, as well, and I'm happy to answer questions about those.

>> BILL PRESS: Thanks and we can come back in the question period. Simon please?

>> SIMON JOHNSON: Thanks very much Bill. My name is Simon Johnson and I'm a professor at M.I.T. I used to be the chief economist at the International Monetary Fund. I think the truth in the matter lies in the second half of your joke about why we are here today which is the extent of the profound change. Your timing is impeccable. As Joe emphasized. The science is still evolving, and yet we can already see some pretty big implications. And let me try and tackle or put forward five. I think the right question in this sort of discussion is what is the problem that we're trying to solve? What Joe and Joe told you is there is a new technology, an arguably better still developing technology for organizing transactions in a decentralized manner. Something as fundamental as payments which we for a long time, 600-800 years, have run in a centralized way, through a centralized trusted party, we can now run that in a decentralized way. And Bitcoin is the proof of concept. What else can you do with this? I think you've all picked up on the fact that very large companies of all kinds are investing heavily in this technology. There's a lot of hype. And hopefully we can strip away some of that hype with you today. But I think there's some really important realities changing. The first use case is the most obvious. And the one that I think always comes up at the top of this kind of agenda, which is situations where you have a central authority. It doesn't work very well. It's corrupt. It's not efficient. They screw up in some way. Now we can bypass the central authority. The leading example would be land registries. We've known in many countries land registries don't work well. You can change someone to change the land record, and when political power changes, they can change the land records. Can we now organize land records in a more decentralized fashion? The answer is absolutely yes. On the point of let's not exaggerate and let's not get carried away, there are a lot of other problems with the creation of functioning land registries that are not solved by a block chain or by decentralized technology. But there's no question, we have a catalyst - there's been a change in the conversation. We have a new focus in these discussions, and we'll hear about some of this when we talk about financial markets with R3 in a moment. The second use, which is getting much less attention, but it's extremely timely for you

to think about it is situations where is we don't have a central authority but we have a lot of dispersed records and we want to integrate and manage those records better. We're extremely bad at this. You can look at the U.S. healthcare system and you can look at the V.A. system as even a more painful example that matters a lot to the federal government right now. There's a technology being developed at M.I.T. called Med Rec, which I highly recommend and bring to you attention, which is a decentralized way using a block chain type of approach to manage access to medical records where the primary records have to remain according to law, but you can access them and manage them in a fundamentally different way. You can manage this network in a way that is absolutely inspired by this technology and uses Etherion as a specific technology. The third use case is one where we see big companies, and I should have said we have a very substantial project at M.I.T. working with private sector people on these use cases and trying to think about not who should be the right vendor, or even what technology you should pick, but where is the social impact? And what should we care about from a policy perspective? Supply chain management. How you move goods across borders is a very complicated and messy problem. So in these situations, there is a trusted set of interactions already. The extent of the trust may vary. There is not a lot of automation in this transaction. We move a huge amount of value. We have to coordinate between private sector firms. We have to coordinate with customs. We have to coordinate with freight forwarding we have to have trade finance in this. To the extent that you can run a better functioning, more decentralized block chain, and perhaps we haven't talked about this enough, but a permission to block chain. To be frank, there is a big debate in the community as to whether we should rely on a permissionless Bitcoin type structure, or to the extent that you can build a relatively controlled system with a defended perimeter, and in which there is decentralized interactions.

The fourth use case is real-time interaction. So just picking up the Wall Street journal today, you can see a couple spectacular examples of instances that happened to be in the financial sector, where executives have taken positions that were not in compliance with the firm's policies, and the risk committees didn't know what the people were doing.

So what you have with block chain technology defined appropriately is a way for people to disclose what they're doing and to provide information on an appropriate basis while protecting their privacy, so you can determine who has access to appropriate knowledge about your investment positions. If you're following for example what's happening at Lending Club or Deucha Bank, this is relevant. There is a lot going into developing the ability to audit activities and understand what your firm is doing. For example, risk positions of a financial firm in realtime. The structure changes fundamentally. It doesn't have to flow up through a hierarchy. It can be available instantaneously through access to the appropriate cryptographic keys so you know what positions your firm has done in all its transactions.

The sixth and final use case I would mention is wider use of this technology including for payments is going to allow us to change the structure of contracts in the economy. Puerto Rico has a large debt problem. Puerto Rico offered to swap some of its debt for a GDP index bond in February. The notional value they said was $25 Billion dollars. The creditors said the value of that to them is roughly zero. Why? Because GDP is a made-up number. By all statistical authorities. The creditors have experienced in Argentina and in Greece and Ukraine that these numbers will be changed when it's of interest to change them. What we're discussing today is a different way to make payments and a different way to verify transactions in a decentralized way so it's not a central authority telling you what's happening either the government reporting or a firm reporting. But that data is much more

widely available and contingent contracts, equity type payoffs will become much more broadly available. And the last point I would make, which is central banks, which are an important gate keeper, including in the regulatory situation that Jerry was describing, are I wouldn't say enthusiastic, but they're encouraging innovation in this area because they see us moving away from our current fragilities. But we have a more decentralized financial structure potentially we can have a change in the form of our contracts away from debt to something that is more resilient in the face of shocks. And we may be able to reduce transaction costs in some of our more fundamental financial transactions, which obviously is a very pressing need in many countries. Thank you very much.

>>BILL PRESS: Thank you, Tim.

>> TIM GRANT: Thank you very much indeed and on behalf of the R3 team and our members around the world we appreciate the opportunity to speak in such esteemed company. Thanks to my fellow panelists - you all said a lot of what I was going to say which is very helpful. Your lack of definitions, regulatory questions, financial surveillance, the investment in the space, the hype cycle. Let's not lose sight of the fact that there's huge amount of hype around this. Supply chain, smart contracts, central banks - this is all the stuff we want to talk about. In the next few minutes I'm hoping that I can control this. There we go. I'm quickly going to spend two minutes on each one of these. What is R3? That will be quick. What is a distributed ledger technology and how does that differ from block chain, there is a difference? What is the promise of DLT for financial services and how are we going to get there? That's really the ultimate question at the end of the day if any of this is actually going to fulfill the promise, how to we get there and make this into production. So what is R3? We don't have exploding asteroids. We don't have...I don't have the ability to control this apparently...there we go. But I do have the world's biggest consortium of banks working on distributed ledger technology. We have 50 member institutions right now from all around the world. We have literally some of the very biggest - you recognize the names. The key is we've come together to try and solve problems. We're exclusively developing next generation financial transaction network, and commercial applications, that's the whole point. We're doing that on distributed ledger technology which has a very distinct relationship with cryptocurrencies and hopefully they'll become clear in the next few minutes. So what are we doing from here? We were 50 members as of today. We're growing very fast. Important to note that we're looking to grow to the entire ecosystem of players around the world. So, yes, other financial institutions, for-profit, asset managers, exchanges, market structures, utilities, the likes of Microsoft and IBM and Intel, who we have good relationships with. Small block chain companies, we have great relationships with all of the incumbent startups. But perhaps most notable, as was mentioned before, regulators and central banks, we fundamentally believe as a membership that the only way to get this stuff adopted, the only way to get this stuff in production, and the only way to realize the promise is to work with the regulators and the central banks and in fact that we're doing so in a number of jurisdictions around the world. That is what R3 is in short. What is distributed ledger technology? I'm not going to spend a lot of time on this. There's two kind of key elements of this paradigm that have been mentioned already. We're moving from a centralized world to a decentralized world that has some certain implications in terms of permission versus permissionless that I won't labor the point on. In the old world, Facebook is a great example of a centralized network. All of the data is, in fact, centralized. None of the data resides on the individual computers of the users. On the other end of the spectrum we have Bitcoin and Ethirium which have been mentioned already

which are indeed fully decentralized. Without putting a philosophical stake in the ground, this is the world that we're all debating where we end up and how we realize the potential benefits of this technology. So swiftly moving on, let's just call out a couple of key concepts that hopefully will resonate and you can walk away with these ideas. Cryptography is key as it's been mentioned before. It's a huge part of everything that we are doing. Nonrepudiation or immutability is key. The ability to be able to be sure that the information is real, let's call that truth, as well.
Smart contracts have been mentioned. This is going to be potentially a significant benefit to the entire financial system and beyond. To have automated execution of business logic at its core. Shared ledgers, distributed ledgers, the idea that the right people see the right information at the right time and that it's not decentralized. That's a huge part of this. And consensus. The idea that we can settle upon the truth and the right people can be clear what the truth is. And what is really key and kind of it's been mentioned already is that none of this is new. On its own, none of these ideas are particularly innovative. It's the way in which they've come together that is particularly impressive. If you haven't read Satoshi Nakamoto's paper from 2009, it's a genuinely beautifully written research piece and I would urge all of you to read it. It was like Henry Ford pulling together the internal combustion engine and mass manufacture, he didn't invent either of them, but he pulled them together. And that's an interesting analogy.

This following slide gives you a sense of the importance of the steps that we're potentially moving into. Before the internet, the notion of processing information at its core was done in a way where we weren't sure that everyone was doing it in the same way. So let's take a really simple example which is one company invoicing another company. Company A has a ledger and that has information about who is owed what. You produce a document called an invoice. You send that invoice through some communication mechanism and the reverse happen at the other end. Before the internet, that communication part, that was fraught with inconsistencies. What the internet did is remove that processing component. We've all seen the extraordinary results. The next step is the truth step. It's the step around perception. That fax that got sent over that may have been put into the ledger in the second company may have been put in the wrong way. Therefore we're not sure what is in one ledger is the same in the other. That's when we have the reconciliation issues, and that is what this step is looking potentially to solve. It's allowing us to reach some form of truth. It sounds perhaps a little bit pie in the sky. But that's the gravity of what we're potentially dealing with here.

So one unique approach, and I should be very, very clear. R3 is building technology, but we don't believe there is only one ledger that would ever exist. There will be many that will work together and will need to interoperate. This is just an example of the kind of problems that we're trying to solve in the financial sector. Our approach is called Corda. The key parts are we don't think you need to share all of the data all of the time. Certain other paradigms do have all of the data, all of the nodes, all of the time. Financial markets and institutions don't believe that to be necessary, so that's a key design decision that we've taken. We've designed this with regulators in mind. We are fundamentally a regulated industry. Globally we don't believe that we're going to get away from that. We don't believe it's a bad thing except when it comes to capital that we might have to hold. This is designed with regulators in mind such that regulators and anybody else who needs access to information will always have access to that information. Legal prose. We're already getting to the point in this march towards reality that we need to be sure that smart contracts actually represent something real. In some respects, smart contracts is a bit of a misnomer. It should be really smart logic. It's a smart contract when there's legal prose in there and it has some contractual basis in reality. I'll move on from this

page. The idea is to give you a sense of the kind of problems that we're definitively trying to solve as a group.

What is the promise of this technology? What is it going to do? If you ask around, you'll get pixie dust and unicorns will be waved and in a couple of years we'll be saving hundreds of billions of dollars and all kinds of new business models will sprout up. The truth is, it's going to take a lot longer and a lot of collaboration, but if we do it right, because this slide is just one small slice of the number of use cases that could be applied. Simon went into some of these. I'm not going to go into all of them. But the point is for financial institutions, for regulators, for individuals, and beyond finance we're aware, we're focused on finance, but beyond this, this technology has potentially significant implications for reducing costs and increasing business opportunity.

Another way of saying it is we're going to reduce operational risks and increase efficiency. Reduction of manual and error-prone processes.
Think of that example that I mentioned earlier on. The ease of validation of financial transactions through smart contracts, that's already been mentioned. I think that's intuitively very clear. If we can make it work, it would be useful for all of us. The real-time legal entity, auditor regulator access, the market surveillance part that Jerry talked about - very much front and center. And knowing your client. Knowing identity, knowing who you are. This has very real implications beyond finance in terms of identifying individuals and companies and other entities. So the benefits are potentially huge.

I'll finish very briefly if I can get to the next slide.
I'm going to skip a couple. Because I realize I'm running out of time.

Where do we go from here? There's a couple of slides on the Lehman crisis which definitively could have been avoided had we had this paradigm. These are the big design challenges that are left for us to solve. Let's not pretend that we've solved them as an industry or technological community. We need to know how everything is going to interoperate. We need to know how to scale this stuff so it operates at the scale that we need at an enterprise level. It has to be secure, private, and identity, and systems integration. The point is none of this has been solved yet, and we're working very hard and a lot of people putting a lot of time into it. The final point and the final slide is to simply say the only way to do this is through collaboration. If I can get to that final slide. There you go.

Our fundamental philosophy is to bring everyone to the table and work together. We're working on a lot of live projects with everybody you see on this slide. We have a lab and research center that we want to work with academics and governments, as well, and ask the questions and solve them and have a road map to the future. Thank you very much.

>> BILL PRESS: Thank you. I see Craig's flag first and then Jim's. And then mine. Craig? And Eric.

>> CRAIG MUNDIE: Thanks, that was great. Joe can answer this question or any of you. I haven't looked at this. A lot of this obviously depends on cryptography. What is the particular nature of the cryptography that is employed now all the way from the identity part to the core of the ledger capability? And what do you see downstream as the issues associated with any vulnerabilities associated with that? Particularly for example is it Quantum hard? Are people looking at that?

>> JOSEPH BONNEAU: Yes, sir, I can answer that. One of the things that is kind of interesting about Bitcoin is that there's no encryption. So you get to sort of skip that whole aspect of crypto. There's really two specific algorithms in Bitcoin which are the workhorse of the entire thing. There's the hash function, SHA-256, which is the most widely used standard. And there's ECDSA, Elliptic Curve Signatures, which are also based on a NIST standard. A lot of times people say Bitcoin uses the same ECDSA that's used in TLS for secure web browsing all the time, it's actually slightly different version that's used in Bitcoin but very closely related technically. So it uses very standard crypto. Crypto algorithms get broken for sure. If you ask me to bet my life that there will be no successful cryptoanalysis in the next 25 years I wouldn't do it. Quantum computers are one way that it might happen, but there are also classical ways that crypto systems get broken. The good news is that Bitcoin and most of these other systems are probably resilient and they're able to change on a several year timeframe. It would be a little bit of a leadership challenge that I'm not sure the community is totally up to right now. But if you told me that these systems, these underlying cryptographic primitives would be broken two years from now we could roll over and switch in that time period.

>> CRAIG MUNDIE: Assuming you had one to switch to.

>> JOSEPH BONNEAU: Yeah, exactly. The post-quantum cryptography is a major research challenge for a lot of the crypto research community right now. NIST is going to run a competition, and in five years we'll have some standard post quantum signature algorithms. In the event that quantum computers start getting closer, and it's going to be, we're very far and there's going to be a lot of milestones that we're going to hit along the way and we'll get a sense that they're closer. It's very unlikely that one will be invented out of scratch that works six months from now. Yeah. Given a few years of time to switch, it would be easy to migrate. So of all the problems in Bitcoin, I think catastrophic cryptographic failure is low on the agenda.

>> SIMON JOHNSON: We should make everyone aware that a lot of the Bitcoin mining takes place in China, about 40% is one estimate. And there are also concerns that the mining pools, well they are certainly more concentrated than the original aspiration which is run on a decentralized system. So this is separate but perhaps not ultimately unrelated.

>> JOSEPH BONNEAU: That would be true no matter what cryptographic algorithms we use.
It's just a matter of where is the electricity and computer chips are cheap build and run.

>> CRAIG MUNDIE: Just one follow up, the real issue in my mind if I believe everything you said, once you get these things deployed at scale, how you transition from one generation to the next is very, very tricky. So while conceptually it's easy, okay, we'll do version two and it will have this other algorithm, how you get all the assets from one to the next also seems like it could be tricky.

>> JOSEPH BONNEAU: Yeah, there is a way to do it. Within any Bitcoin or any other crypto system, we would have a new type of address that you would send money to that would represent a public key in a new signature algorithm. And there would be basically be a time when you say change from the Franc to the Euro, you have to say, you know, you have two years before you have to change to the new thing after which, in this case, it might be dangerous to keep it around. There are some old systems that may never move it over and maybe they'll get attacked, but hopefully the majority of people will change over in due course. But yeah. The problem is not so much formatting and having a

way to do it, there would be some tail of people that just never upgrade and probably lose their money when the crypto system is broken.

>> TIM GRANT: Perhaps just to add another angle to that, obviously we represent however many billions dollars of IT spend across the world in current, engrained legacy systems. It's definitely true that it's more challenging to innovate when you have decades of technological debt to fight against. And that's why in R3 and I think in the community as a whole there are more players than just R3. We have to think about systems integration and that changeover now. Not in five years. And we build that into the plan. Otherwise we will simply not be able to do it. And large institutions won't make that call. It's just too expensive.

>> CRAIG MUNDIE: Even facing the cyber threat, the banking industry hasn't been managed to get itself out of that. And a forced function transition due to an unexpected transition here I think would be even more challenging. I encourage you to think about that.

>> JOSEPH BONNEAU: I can add one more quick note, which is to say we've gone through this on the internet many times. We tried to transition away from MD5 and SHA-1. Those have both been very disappointing. They've been very slow to move. Browsers have tried to force websites to stop using these so that they can turn it off and people have always dragged their feet. But I do think the economics are a lot different in cryptocurrencies. It's not a matter of somebody telling you we'll cut off access. It's a real threat saying your money will be gone if you don't switch. So hopefully all of the different parties who need to switch will do it, as opposed to people who don't want to reinstall some new software on their web server because they don't think the browser manufacturers are going to cut off service to them.

>> CRAIG MUNDIE: But once you move away from currencies to land records and everything else, those incentives become highly variable and people's ability to process it will be highly variable.

>> BILL PRESS: Okay, I'm going to move us on. Very interesting point. Jim Gates is next.

>> JAMES GATES: Thank you to the panel for the briefing. This question comes in response to a comment from Tim. You mentioned the Lehman Brothers incident shall we say. I'm no financial expert. But most crashes in my study of them seem to follow a general pattern which is they're about extrapolations into the future and that's where you lose value. From the Tulip crash in the 1600s to our market crash in '08, it's always the same pattern about creating financial instruments based on projections into the future that don't bear the value that they're projected. So how does a cryptocurrency break this cycle?

>> TIM GRANT: That's a good question. I appreciate that question a lot actually. I will speak from some degree of expertise, having been a guy at UBS, which was one of the biggest losers of the crash who got the call on Friday the 14th of September from the group CFO and CRO saying please tell me what our exposure to the Lehman Brothers is. That was a long weekend with very limited sleep. But the reality is that took me and a large team 48 hours to figure out what that was. And by the end of that weekend, we had nothing more than a basic spreadsheet to tell us what our exposure was in multiple billion dollars to one of the biggest financial institutions around. So really I think we divorce the market forces and the exuberance and the expected versus the realized value from what happened

next.
And if we were all able to have a real-time, completely transparent perspective on what our exposures were to everybody, we would have been able to unwind in a much more orderly way and it would have saved us a lot of money actually and potentially could have saved Lehman from going down. A lot of what affected Lehman and other big financial institutions is they didn't know what their exposures were. I don't think that's uncontroversial eight years after the fact. I've seen it firsthand. Boy would I have liked to have that button that I could have pressed on September 14th of 2008 and had the answers.

>> JAMES GATES: I still don't understand how that impedes the creation of these fraudulent financial instruments?

>> TIM GRANT: It doesn't. Probably there are elements of that. But the way it could have avoided the Lehman collapse, which was the statement I made, were a block of other institutions took the same bets and didn't collapse obviously. In that particular case I think they made some strategic decisions at broad level that put them in a slightly worse situation but had they had the kind of level of transparency, aside how it all got to that point, it may not have gone down. I think that's a fair statement.

>> SIMON JOHNSON: Mr. Gates, I rather agree with you. I think this will mean big changes for finance and you should follow carefully the Lending Club Scandal, and how you could organize that information differently and how if it was managed differently within the firm with supervisors we could have a better structure. But I agree with you - and I was the Chief of Commerce in 2007 and 2008 and none of this is my fault. I should have said that at if beginning.
(Laughter). But you're right, the boom-bust cycle is not going to go away but we're going to change the nature of it and we're going to change the winners and losers, but that cycle is going to be with us.

>> JOSEPH BONNEAU: I can just add there have been numerous examples in the cryptocurrency space already, huge speculative bubbles that have already popped. Lots of different alternative currencies to Bitcoin that were proposed went way up in value and then people realize there was no innovation and it collapsed. So it's happened again and again. People have invented lots of new ways to have bubbles within Bitcoin or other cryptocurrency things. Human nature of people wanting to invest in the next big thing is never really going to change.

>> BILL PRESS: Good, Eric?

>> ERIC LANDER: I was curious about the brief mention of medical applications and how this was going to change medical records. I was wondering if you could say a little bit more about that.

>> SIMON JOHNSON: This is an innovation for M.I.T., Andy Lipman's group at the media lab. It's still under development. I think it's absolutely fascinating. We don't have a central authority that's not functioning. We don't have anything in the middle. And we know what we need to be able to call upon records, have people with appropriate authorization be able to look at them and integrate that information. But we're also not allowed to move data. It would reside where it currently resides, which is mandated by law. I will send you the information we have on Med Rec at M.I.T. And I would suggest that Andy follow up with you and your team. I think it's highly relevant to all the things that

you work on for example.

>>ERIC LANDER: Please do, thank you.

>> BILL PRESS: My question, I guess it comes from something that Jerry brought up. At the consumer level use of this, somehow Jerry was trying to make a distinction as to whether it's value was housed by an intermediary or on my computer here. But I don't understand that because my computer here is constantly in contact with the web. It's doing negotiations, it can be hacked. I don't understand a fundamental distinction between hacking my bank and hacking through my bank to the computer. It's another tentacle of the octopus. And another way of stating the question, I may think I have a wallet on my computer, but I as a consumer have no way of doing independent cryptographics checks to see if it's long since already stolen my Bitcoin and simulating the transactions in a kind of Ponsi scheme. It does pay my people, but when zero day arrives, everybody loses their money. I wonder if you can say something from the naive consumer side?

>> JOSEPH BONNEAU: Sure. I guess I can say in general it's very hard not just for consumers, but for expert computer scientists to be sure that a computing device that they are holding actually does what it's supposed to do. We basically never solved this problem and there's reason to believe that we'll never completely solve this problem. It gets into this trusting trust. Who made your computer? Who compiled the software that's running on it, etc. It sort of never goes down. When we're doing computer science research, especially security research, we usually assume some trusted computing base that you hope is behaving correctly. It's probably fair to say that your laptop is probably too big and we don't know how to deliver to consumers' laptops that they can trust are behaving exactly the way they are supposed to. There have been some alternative solutions for Bitcoins specifically that try to fix this. There are a bunch of different companies that sell small, special-purpose hardware devices whose only job is to keep your Bitcoin keys safe and have some small interface for you to authorize sending and receiving money. And the hope is you buy this specific device. You can't install apps or malware and hopefully that will be a good steward of your cryptokeys that you can trust and put in your pocket. But in general we hope you can run some software that will maintain your key, but that's been an unsolved problem in computer science for a long time.

>> JERRY BRITO: And I think what you're getting at is, are you moving the attack surface to somewhere else. But you're for the first time creating the ability for consumers to hold their own funds, which wasn't possible before. This opens up a whole host of new possibilities. I think in the developed world we lose sight of why this is important because we have very good trusted financial intermediaries that we can use. And when we deposit our money there, we know they're typically not going to go away. We know that our currency is well managed and isn't going to be inflated away. And we know that if there is a hack, we're probably going to be made whole. In other parts of the world, that's not the case. So there is for consumers a real value to having the ability to hold value for themselves. And to accept value directly. So in many parts of the world, just staying to the narrow payments application, which is just one of many applications of this technology. In many parts of the world, there is no good way to accept electronic payments. In fact, it was brought to my attention recently that Paypal does not operate in Puerto Rico. So in Puerto Rico you could not use Paypal. But Bitcoin is something that all you need to use is an internet connection, a device, and free and open source software. You're right that you are always going to be potentially subject to attack, but you have new capabilities that you did not have before as a consumer.

>> SIMON JOHNSON: Bill, I think the future of money largely depends on what the central banks are going to do. And I think the central banks are going to worry about what you're worried about. And while the future of money is absolutely digital. And from a consumer point of view, they don't know or care how that digital representation actually operates. I think the extent to which we actually use Bitcoin literally in our monetary transactions will be relatively small. I think this block chain technology has massive other profound implications. Bitcoin at least brings very healthy competitive pressure onto the banks and onto the central banks to up their game. They're way behind in applying existing technology and improving how the systems work. I also suspect also linked to the point that Craig made in terms of the vulnerability of our systems, I think the central banks are going to shy away ultimately from the pure cryptocurrency solution.

>> JOSEPH BONNEAU: I totally agree with Simon. The impact of cryptocurrencies as daily use consumer payment systems is usually overstated. I think most of the banks are going to be elsewhere. But I want to challenge something Jerry said about how the ability to keep currency to yourself is something fundamentally new that cryptocurrencies are delivering because I could withdraw all of my personal savings as cash from the bank and put them in my freezer if I wanted to. And most people would tell me that's a bad idea because then I could lose everything if a burglar breaks into my home. To me, the analogy is not perfect.

>> JERRY BRITO: I should have qualified by saying in electronic fashion.

>> JOSEPH BONNEAU: Right. The difference is you can put your whole net worth either on your laptop or in your freezer or wherever you'd bury your cash. And in both cases there is always a risk in holding it yourself or lending it out to a bank that might lose them. The difference is that in some developing countries, there aren't really great options for putting your funds in a financial institution that's trust worthy. In the west, bank robberies have become a lot less rare so they are not something that are on a lot of people's radar. And in the cryptocurrencies space, exchanges are much more likely to fail so the balance of probabilities of keeping you funds yourself vs. loaning them out is a little different.

>> SIMON JOHNSON: I think this is the key point, if I may, because what is cash, cash is this token issued by central banks. It has no value except what people think it's worth. And what is the fall back in other countries? U.S. dollars cash. That's where most hundred dollar bills are held. What the central banks are grappling with is they give you this non-digital piece of paper. They don't give you access to what they could, which is a digital token. Liability of the central banks - that you can only have through the private commercial banks. The central banks are trying to figure out how to change that and how to give you a robust digital token that could be used globally and you can argue about how that system runs. I don't want to say they want to keep the banks where they are, but they are worried if they do that in a very rapid way that could be disruptive and that could generate all kinds of issues in, for example, how the credit system operates. But that appeal, this Joe-Jerry discussion here, that's exactly what the central banks, the big ones in the leading countries around the world are grappling with right now.

>>BILL PRESS: Eric Lander, last question.

>> ERIC LANDER: I'm following this discussion. I'm not sure I've got all of it but I'm getting very worried

about somebody stealing my Bitcoin or the thing in my freezer or wherever it is. And it occurs to me, is there some way, maybe this is not a well-posed question, but where my currency can be distributed across multiple places so if it gets stolen from not too many of them I still have it?

>> JOSEPH BONNEAU: Great question. The answer is yes there is.

>> ERIC LANDER: I would like to do that. If you could work that out with me after this session.

(Laughter).

>>ERIC LANDER: I want the same dollar in multiple places so that dollar can't get lost. How do I do that?

>> JOSEPH BONNEAU: What's interesting, I think this is something that is fundamentally new about cryptocurrency. Even dating to Bitcoins, it's built into the Bitcoin design and every system since. That coins can be assigned to some quorum of keys. So you can say, here are three cryptographic keys and if any two of them agree to send the money, than the money is sent. Unlike with cash, which you can't really split. You can put your cash in three different places and if one of them gets stolen, you'll lose a third of the cash. With digital currencies, you can put your keys in three different places and if any one of those keys gets stolen, you're still secure. It doesn't have to be two out of three, it can be any number out of any number. It's been a research project at Princeton to streamline that technology and make it more efficient. Glad you asked because we've been working on it. That is very exciting and there are a lot of different models that have been propose that had don't really have good offline analogies. You can use an intermediary and you can have them hold a key and you also hold a hardware key locally. And this poses a lot of regulatory challenges, too, because most financial regulation is based around the concept of a token being in some physical location. That is no longer necessarily true.

>> SIMON JOHNSON: We used to believe in this country that people should sort this question out for themselves. And what we learned in the 1930s is when this privately determined system breaks down, the government has to get involved because it has massive negative effects on the economy. So we have the FDIC and if any of these private arrangements becomes big, at scale and it breaks down the government has to get involved. And so we better know what that means. And what the backstops are if we're moving away from what we have now, which is not a great system, but it does have some robustness on points like that. Is the retail investor protected and do they feel secure. Even in the height of the crisis in 2008, retail depositors did not run, did not try to withdraw their deposits from their banks which is a remarkable achievement.

>> TIM GRANT: To punctuate the point - we haven't made it as a panel so perhaps to actually say it out loud - as we move from the old paradigm to the potentially new paradigm, we're going to have to represent Fiat currency on this system somehow. And that fiat currency is going to have to be distributed and exchanged in a way that we are all used to having certain risks and custodial custodies that we need. That isn't going to go away and so we still have to solve for those problems. So central banks, as Simon rightly points out are actually thinking about this. Regulators are actually thinking about this and the only way we get there is if we work as one ecosystem, otherwise it ain't gonna fly.

>> CRAIG MUNDIE: It's interesting, the FDIC was deposits. And now there aren't any, but you're going to still have to have the same ability for the government to stand behind it.

>> BILL PRESS: D will stand for digital in some way and we'll have to work out the other three letters.

>>SPEAKER: I think the whole thing sounds like Shroedinger's Cache to me.

>> CRAIG MUNDIE: B for bits.

>> BILL PRESS: We've run over because it's been such an interesting session. But why don't we thank this panel now.

[Applause]

Public Comment

>> JOHN HOLDREN: And we now move to the public comment portion of the program. I believe there is just one public comment. Maxine Savitz will preside.

>> MAXINE SAVITZ: Thank you, John. As Dr. Holdren mentioned in the beginning of the meeting, the PCAST has several studies underway. And one of these has to do with how science and technology can be used to ensure the safety of our drinking water.
And the one public comment that we have today is from Dr. William Hirzy. I know he will be settling in, in a minute.

Okay, welcome Dr. Hirzy. He is the Science and Regulatory Affairs Advisor to the American Environmental Health Studies Project/Flash Fluoride Action Network and he's going to be talking about lead in drinking water and increases in children's blood levels. As you know we have a two minute rule and we'll let you know in 90 seconds.

>> WILLIAM HIRZY: Thank you very much. I'm also a retired senior scientist at EPA headquarters here in D.C. and charter member and past president of the Professionals Labor Union at the EPA, and this issue came to my attention while serving as the union officer. Honorable council members, thank you for the opportunity to bring to your attention the material that's germane to the lead in drinking water issue which is of considerable interest to Congress, public health professionals, and the public at large. There was a recent article by Brady Dennis in the Washington Post which addressed this issue focusing on problems with the EPA lead and copper rule. But unmentioned in this otherwise comprehensive piece is the relationship between lead leaching in the drinking water, and the chemical used in 90% of fluorinated water systems - fluorosilicic acid. This relationship has been known by EPA, local government officials, and others in the public health community for over a decade, but it has not been acknowledged nor acted upon in spite of its significance. I can't provide a detailed treatment of this subject in this brief time I have today, but one is available, written by Michael Connett and is at the URL that appears in my written comments. Peer reviewed publications cited below and discussed at length in the Connett article have pointed out that fluorosilicic acid is a potent leacher of lead from leaded brass plumbing fixtures and lead service lines and its use in fluoridation systems increases blood lead levels in children compared with an alternate fluorinating agent sodium fluoride or in children

drinking unfluoridated water. Given the widespread existence of lead service lines in communities using fluorosilicic acid it would be a simple expedient for lowering lead leeching and children's blood lead levels to stop adding that particular chemical to drinking water, whether or not anticorrosion measures such as the addition of zinc phosphate are in place. After all, lead phosphate particles can and do release from the deposited solids in these service lines and find their way into drinking water at the tap. It's better not to have lead leached from the metal in the first place. I would be happy to answer any questions.

>> MAXINE SAVITZ: Thank you and you have provided references. Thank you very much

>> JOHN HOLDREN: That brings our program to a close. Again, thanks to the PCAST members, thanks to the panelists, and our one public commenter, and thanks to the audience, both in the room and over the web. And of course, thanks as always to our able PCAST staff, including particularly the PCAST secretariat who organizes these meetings. We are adjourned.