Mr. PUTNAM. Thank you very much.

Let me begin with a question for you, sir. How many ballot questions will fit on the card that you held up?

Mr. MORGANSTEIN. Well, I have a lot of jokes about the city of Chicago, and I come from that city. And when I tell those jokes to people who are election officials there, I get into trouble. The typical Chicago ballot will have 75 judicial retention questions whereby judges are up, and you probably aware of that, sir. We have programmed an election for the city of Chicago—we programmed the 2000 election in which there were some, I think, 96 ballot questions, counting 75 judicial retention, President, Vice President, and so on. And that is, as a matter of fact, the limit that we can put on here. We can put 96. You can have thousands of people on the ballot, thousands of questions, but 96 selections, which is more than adequate for any election we have seen.

Mr. PUTNAM. So that being the ballot, the voter can read their 96 selections on that piece of paper?

Mr. MORGANSTEIN. Yes, sir. There are two ways the voter can do that. It is printed in a human readable format. You can see some numbers—and I am happy to pass these up to the committee if you would like to touch these.

Mr. PUTNAM. That would be helpful.

Mr. MORGANSTEIN. There is a human readable portion on the bottom, and then you see a bar code in there, which as the last time you went to the supermarket to buy a can of soup, you know that it read the price properly. The voter can hold that underneath a laser beam, and in the privacy of a voting booth it will show the selections, English selection, President of the United States and so on that they have picked up to 96.

Mr. PUTNAM. Dr. Shamos, considering the pool of people able to hack into electronic voting systems is presumably smaller than those who are able to do it the old-fashioned way by manipulating the paper system, would you agree or disagree that electronic systems increase security of the ballot?

Mr. SHAMOS. Properly designed and properly deployed and tested systems, DRE systems, do indeed increase the security of the ballot.

Mr. PUTNAM. Dr. Rubin, after volunteering as a poll worker, you were quoted as saying that the experience showed you that one potential attack would be far more difficult to pull off than you and your colleagues had assumed. Is that an accurate quote, and do you still feel that a serious attack is likely?

Mr. RUBIN. Yeah. It's not a misquote, but it's the first half of a sentence where the second half was, "I have found some attacks that I considered would have been harder to pull off in my precinct. I thought of new ones that I hadn't considered. And basically I think the experience focused me better on appreciating what the real risks were," and at the end of that paragraph, I stated that I still believe that these were a fundamental risk to our elections.

So I did not believe the system was any less secure after working there. I just sharpened my appreciation for the various attacks.

Mr. PUTNAM. Is it more or less difficult to perpetrate fraud using electronic devices over traditional paper ballots?

Mr. RUBIN. I believe it is probably more difficult to perpetrate fraud, but that the fraud would have much more far-reaching consequences if it were successful.

Mr. PUTNAM. And for the short term, this whole idea of a paper trail, is it technologically feasible to deploy an auditable, verifiable paper trail in every machine in America between now and November?

Mr. RUBIN. I don't know.

Mr. PUTNAM. Anyone else?

Mr. SHAMOS. It is not possible.

Mr. PUTNAM. Mr. Adler.

Mr. ADLER. It is not possible.

Mr. MORGANSTEIN. I would be wealthy if it were true, but it is not possible.

Mr. PUTNAM. So we are all in agreement, with the exception of Dr. Rubin, that this is really a discussion about improving or changing or altering the approach for the 2006 election, because 2004 is out.

Mr. MORGANSTEIN. There are primaries in 2005, and there are municipal elections in 2005.

Mr. PUTNAM. OK.

Mr. RUBIN. I will agree with that statement, too.

Mr. PUTNAM. OK. So this is all then, about post-Presidential election and the challenges that we are going to have to deal with. We have heard testimony that no system is perfect, they all have their problems, they all have their security issues. We all deal with a certain amount of error every day in on-line IRS filings, ATM machines, self-serve gas pumps that scan our credit cards, and we all deal with a margin of error in electronic devices involving our finances. And obviously voting is a fundamental piece of our democracy, and we ought to do everything we can to secure it as well.

But my concern is that this election is going to be seen as being a fiasco despite the fact that there may or may not be any greater error rate than historically has been the case because of the sensitivity, the international scrutiny, and the fact that now, frankly, both parties are ramping up teams of attorneys to figure out ways to exploit what everyone admits is an imperfect system.

So knowing that everyone, the first panel and I believe all of you are in agreement—and if you are not, please say so. Knowing that everyone agrees that there is a margin of error in every single system deployed, how do we develop some standard that defines an acceptable error rate, knowing that this thing is going to be litigated and played out both in the media and presumably in the courts again? How do we have some standard if everybody agrees that there is going to be something that someone can point to and say that is an imperfect system? Because we haven't designed a perfect one. What is the definition?

Mr. Morganstein, and we will work across the table.

Mr. MORGANSTEIN. Thank you, Mr. Chairman. I will be brief. I was very honored last week to participate in a panel at the National Academy of Sciences right here in Washington with some of the smartest people I have ever seen or had the pleasure to sit down next to. And evidence was presented, sir, that showed that the voting system unquestionably counts. It makes a difference. It

lowers error rates. Unquestionably. If you start from hand-marked ballots, which sound simple—make an X; well, some people make a circle and other things happen—to punchcards, which were good for a long time, and then we saw, well, maybe not so good; to optical scan that provide feedback to voters in the precinct. Better yet. And you can see that when we did these, the questions on the ballot didn't get easier, but the technology got better and the error rates did increase.

I think DREs are a step further yet, and a I think a voter-verifiable touch screen—which is not really a DRE, by the way—is yet another step.

The answer, sir, to your question is, like anything else that we have done in this country, we have recognized the importance of continual improvement. It is not like the Constitution says, a more perfect union; you know, it is something perfect, you can't make it more perfect. We are getting better and better, and that is the best we can do as humans, is make it better and better and work on continuing improvement.

Mr. PUTNAM. Mr. Adler.

Mr. ADLER. As Dr. Shamos said, there is no election science, and we—the election community—are making it up as we go. And that is just a true statement. On the committee that I co-chair at IEEE on voter verifiability, we have put out margin-of-error levels, standards that every system should meet, whether it be paper DREs or receipt-based systems where you can spot check these things.

Statistics govern our whole lives. How do you know that a vaccine works? Because you didn't get sick? If you didn't take it, you might not have sick either. We do statistical analyses in this society that we base policy upon. What we are not doing with voting is we are not measuring the margin of error. The first thing we have to do is measure it and figure out how to measure it across systems, whether it be DREs, whether it be paper ballots. And I think once we understand that—and we have done some analysis which says if 2,000 people faithfully spot check and verify their vote, actually counted properly in a congressional district of, say, 400,000 voters, you can get a margin of error that you can take to court that is about a quarter of a percent. If you want better than that, you need more spot checking.

And that is exactly what we did with lever machines; we used to spot check them. There was no paper to recount. We had a meaningful audit trail. And there are performance requirements that we need to institute and measure for every system on Election Day that will provide the second component, which we have all talked about, which is voter confidence. I get a receipt at the gas pump if I want it. If I get a receipt at the voting machine—in our focus groups, and we put about 70 people, you know, through our last incarnation, whether they were going to check or not, they said I would rather have it than not have it.

Between those two, measuring and giving the voters some confidence their vote counted and some proof their vote counted, I believe, is a way forward.

Mr. PUTNAM. That technology test that would give you that .25 margin of error, isn't it true that would not take into consideration a confusing ballot design that, frankly, in Florida was one of the

key reasons for voter confusion? But technically the machine worked. They were overvotes as a result of voter confusion on a complicated design. So, I mean, that is the whole other human piece; right?

Mr. ADLER. Well, I would agree that the most difficult place is between the voter's gray matter and how they represent it. And we have done a lot—the best things DREs do is stop overvotes. Overvotes have gone to zero. And so we will continue to deal with that gap, from gray matter to medium.

The question that I think we are all dealing with, and actually NIST put out a report on usability, is once the voter intent is captured, how do you make sure it is counted accurately or properly, faithfully? And then the chain of custody all the way to rolling up the result. You have to do it from gray matter all the way to results, and that is the end-to-end solution or end-to-end system that we need to measure.

Mr. PUTNAM. I will let the other two finish, and then go over to Mr. Clay.

Mr. SHAMOS. I have to make the question more complex before actually giving an answer. We have no definition of what error is in voting. Political scientists think it is an error when a voter goes into a voting booth and comes out without having voted for every race and question on the ballot. They actually use the word "error" in reference to that. Error can occur because of a difficulty in a voter expressing her choices. That is, they have in mind a certain slate they want to vote for, and it ends up, through error or mistake in the voting booth, they don't actually end up voting for those people.

Then, of course, there is the issue of error in the software, error in the hardware, that may cause the vote to be recorded differently from the correctly expressed intention of the voter. But even if that could ever be reduced to zero, which it can't, that still doesn't mean that we have error-free voting, because the votes must be totaled, the totals must be communicated through a central place. We must make sure that every voting machine that was used, that its totals are correctly reported and added together. And so there are many parts in the process which have the potential for introducing error.

The issue with paper, paper receipts and paper trails, is exactly which of those errors they address. And they do address one error very well; and that is, the error in the voter communicating her choices to the machine. When the verified piece of paper or whatever mechanism is used—and there are numerous ways of verifying ballots without using paper. Whatever the mechanism is used, it does provide an instantaneous feedback that, yes, the machine heard me correctly. Unfortunately, because of the inability to secure the physical custody of ballots—these, after all, are potentially touched by 1.4 million poll workers around the United States on their way to the central counting station. Despite the fact that the voter was heard properly, it doesn't mean that piece of paper is ever going to be around for a recount, that it will not have been augmented, destroyed, modified, or changed in some other way. That is the fundamental problem with relying on paper.

Mr. PUTNAM. Dr. Rubin.

Mr. RUBIN. My area of expertise is computer security. That is what I do for a living. And so I face this question all the time because no system that is on is secure. And in my consulting work I am often asked, we want you to help us design this or evaluate it to make sure it keeps hackers out, and that we are not vulnerable to data loss. And I say it can't be done.

So given that, the goal is to make things better and to make them as secure as possible. You know, I talk about spectrum from really insecure to very, very good. And you try to fall in the best possible spot on there.

I think what we need to do is use all the technologies available, whether the modern and computerized ones or the old paper ones, utilize the best properties of each, and make the system as good as possible and then hope that the election is not too close.

Mr. PUTNAM. Mr. Clay.

Mr. CLAY. Thank you, Mr. Chairman.

Dr. Rubin, the debate about improving the security and reliability of the electronic voting machine has up to this point focused on the use of a voter-verified paper audit trail. While the idea has many supporters, others say that moving toward this sort of paper trail is impractical and may prove unwieldy. In your opinion, are there any better solutions?

Mr. RUBIN. I believe that 20 years from now we will all be voting on systems like Mr. Adler's and David Chaum's, and universal verifiability. I think that cryptographic solutions hold a lot of promise.

I approached this from the point of view that many, many places are using DREs. And I got to see one of those DREs inside, and I believe that systems like that, that are fully electronic, that don't have the cryptographic protections cannot be relied upon without a voter-verifiable paper trail.

Mr. CLAY. Dr. Shamos, you said, "The system that we have for testing and certifying voting equipment in this country is not only broken, but it is virtually nonexistent."

Given that situation, should we have a moratorium on the purchase of new DRE equipment until we have adequate standards and an adequate certification process?

Mr. SHAMOS. I am thinking.

I have never met the question in that form. There are good DREs and there are bad DREs. And the problem is, the public doesn't know which is which, and often Secretaries of State don't know which is which because of failures in the certification process.

As Dr. Rubin pointed out, the systems that we have that are known to have serious security flaws all passed the independent testing authority certification process or qualification process and were actually adopted by a number of States. The issue with moratorium—I mean, I pointed out before that we haven't had a verified incident of tampering with a DRE machine in the United States. That doesn't mean it doesn't occur and it doesn't mean that it won't happen tomorrow. Except that when we are trying to safeguard against risks, we tend to focus our attention and money on those risks that have occurred at least once.

And so the answer is, if we know that certain machines have security flaws, for example, the ability to plug a keyboard—conceal a keyboard on one's person and plug it into a voting machine in

a polling place on Election Day and type things in to modify the contents of the machine, a grotesque security flaw. Nonetheless, there are safeguards that can be introduced to prevent anybody from actually doing that. If it's necessary to put people through a metal detector or watch them as they are going in and out of the booth, then we do that. And so I don't think the moratorium is the right answer, either, because it condemns us to live with the worst systems of the past.

Mr. CLAY. Thank you for your response.

Mr. Adler, can a computer be programmed to show one thing on a screen and record something else on an electronic device?

Mr. ADLER. I think the statement you made earlier about trust and verify applies. Yes, a machine can display one thing and record another. Just like even with the voter-verified paper ballot, it could record one thing electronically, print it on the paper, and hope the voter doesn't see it. And if I could give you one parable about how this might work.

My 64-year-old mother lives still in Florida, Tampa Bay area. She has been using these machines for the last 4 years. Loves them. Said: Mom, they are going to put a paper ballot next to it; you are going to have to compare them; and, if they are right, you press the button. She said, first question: If I don't compare them, will my vote count? And I said, of course it's going to count. She said, then why would I really do it? I am touching the screen.

Now, here comes the recount where the paper ballot and the electronic ballot box do not match. They are going to bring people like my mother into court and say, ma'am, did you look at that paper ballot? She is going to say, no, sir, I didn't think I needed to.

So is it voter verified? Is it a source document prepared by the voter, and can the system do exactly what you said: put one thing on the paper, put one thing electronically, and hope the voter doesn't see it?

Mr. CLAY. Let me ask you, did your company consider producing a voting product on the Internet?

Mr. ADLER. Yes, we did, and we do.

Mr. CLAY. And your company experienced an Internet attack? Do you feel the Internet is a safe place to vote?

Mr. ADLER. I think anyplace you use electronics, you must verify. And, again, it's not really about the hackers. With voting, we don't know where the bad guys are, depending on where you are politically sitting.

Mr. CLAY. OK. My time is up. Let me ask you, why should voters trust a company? This is not malicious in any way to your company, but why should voters trust a company that could not protect their own assets from attack over the Internet when they say they can produce a paperless voting system that is secure?

Mr. ADLER. They shouldn't trust anyone when it comes to voting. That is one of the reasons why we published our source code, we published all our mathematics and algorithms, protocols, we patented all our technology; which means it is published. And every election, all the data that comes out of this machine is verifiable by anyone. You shouldn't trust me, you shouldn't trust the local election official, you shouldn't trust the parties.

As Congressman Holt said, the voter can verify their vote, and we need to give them the means to do that, not just that it was recorded but that it was properly counted, and let anyone verify the results. No one should be trusted in voting. No one. Not the company, not anyone else. And we at VoteHere are dedicated to that. So that if something did happen—the worst catastrophe of a democracy is an undetected fraud. A detectable fraud is embarrassing and expensive, but recoverable. And we need to have the means to detect fraud when it occurs, and we are dedicated to that.

Mr. CLAY. Thank you for your response.

And Mr. Morganstein, why did your company choose to have paper ballots printed by your voting system?

Mr. MORGANSTEIN. We were asked to do that by an election official in our State—if it plays in Peoria, in fact it came from Peoria—by an election official who had been working in the field for some 20 years, who said, you know, I like this touch-screen idea, but there is no audit trail. And I was fortunate enough to have some other successful inventions, and they asked me to put my mind into that and that is what resulted.

Mr. CLAY. Thank you for your response.

Mr. Chairman, I yield back. Thank you.

Mr. PUTNAM. Ms. Kaptur, you are recognized.

Ms. KAPTUR. Again, I just want to thank the chairman, Mr. Putnam, and the ranking member, Mr. Clay, for holding this very important hearing. And so many Members are interested in this, and obviously our citizenry is interested in this issue of security of the vote.

I wanted to ask several questions, and I hope I can get through them quickly. One of the counties I represent, Lucas County, has a situation where they were going to bring on Diebold technology. And the Secretary of State has just said that is uncertified and has taken it off the list. And some of our counties in Ohio of 88 counties had signed contracts with Diebold. They cannot use that equipment now, as of November. The local county, Lucas in particular, is now being faced with a 300, I don't know, 80,000 bill, I guess, to try to bring on some type of optical scanning equipment by November to try to have the ballots in a situation where we can have a recount. Because, under Ohio statute, you have to be within one-half of 1 percent; if you are, a recount is required. And we are told that in the technologies they have been looking at, that was impossible. So they have to do the optical scan.

What advice would you give to the Board of Election? They are in a tizzy now, saying, well, that the Federal money that is available from Washington that I voted for can't be spent to pay for the optical scan for November. And the county is broke. We have 10,000 fewer jobs than we had 3 years ago. The State is broke. But all this money is sitting there from HAVA. Do you have any advice? What would you advise to our local county? Maybe some of you could give them a better price than Diebold is offering on these Optiscan machines.

Mr. SHAMOS. I would advise hiring a lawyer. It is important in procuring voting system equipment to get a representation and continuing warranty from the vendor that their system meets certain standards and will continue to meet those standards. And if

the system becomes decertified, then the financial burden should be placed on the vendor, ultimately its bonding company, to make good to the county so that it can purchase whatever substitute is necessary.

Ms. KAPTUR. Thank you for that suggestion. Believe me, I will pass it on to them. Do you think it is appropriate for private companies to coach and teach board of elections officials and precinct workers? Or should that training of election officials, which Federal money has been designated for, should that be done by publicly hired workers who work for the board of elections, not for any company?

Mr. SHAMOS. Well, maybe the vendors would want to give another answer. But I don't like it. However, it is almost a universally held opinion among election officials that there is no alternative to it, because there is no other source of expertise about the particular systems that are being used, other than the vendor who has seen them used in numerous jurisdictions, has seen all kinds of incidents and knows to deal with them.

Ms. KAPTUR. Well, this is a very troubling aspect to me, that private companies—Mr. Adler, I was very interested in what you said, that your technology patent was open to the public realm. When I made this statement in Ohio, that if we adopt a certain machine, that should fall into the public domain, there were many who opposed that point of view. You've stated exactly what I think should happen in terms of the technologies that are used: Are they public or are they private? Who provides the training? How do we know what is really going? Who are the experts that end up controlling the election process itself? I guess I am especially protective of the citizens' interests, because in our county, in Lucas County, we have always counted at the precinct level.

When I saw, Mr. Chairman, what happened in Florida, I couldn't believe it, where it take votes to another site, you count the votes. That is no anathema to what we do. It was agonizing to watch, actually. And our elections are very decentralized in my home county. And I am not saying there probably aren't errors, but it really is very democratic, gets right down to the precinct level, results have to be posted, they have to be placed on the outside doors. There are all kinds of things that—you have to have two people from each party, plus a judge, looking over each other's shoulders; and the count, it is very, very Jeffersonian. I mean, it is right down to the grassroots level.

So when I hear about what companies are doing in all of this, I am very troubled. And I wanted to ask you, I read some reports about Georgia in the last election, which said that there is this conjecture, 25,000 patches on machines that were employed in Georgia. What is a patch, and was that done or wasn't it done?

Mr. RUBIN. I will answer that first one. When a program is written, it contains lines of code. This is something that a programmer types in to make the computer do whatever they want. That gets compiled into software which is what runs on the machine. From time to time, errors are found in the software or something needs to be updated or fixed. And this generally occurs across all disciplines when software is developed, and you want to upgrade the software and make it new or change some of it. So you write a patch, which is something
ware. It adds lines of sourc
apply a patch, what you a
sion of the software that is
changes. So a patch can co
ware package. It can make
And I also have read a l
have any personal firsthar
happened. But I would say
that if a patch gets applie
or shortly before, that is n
ferent machine, and it need
And so you need to be v
that you mentioned about a
the vendors. On Election D
with the machines and appl
Ms. KAPTUR. Well, I will
from—and I'm a precinct
Congresswoman—they sent
deal with a scanner that w
cause we didn't have electio
work. And I am thinking, wh
Mr. Chairman, I want to
don't want to go overtime. I
to ask, if you would be kind
Mr. PUTNAM. You have tin
Ms. KAPTUR. Do I have tin
I just wanted to ask you if
nology that Mr. Akin Gibbs
contractors that had a techn
reviewed by the States—the
tions. Do you know, is that t
its name is? He was in the S
Mr. MORGANSTEIN. The Tr
Ms. KAPTUR. I think that
Mr. MORGANSTEIN. That is
Mr. RUBIN. I had read acc
in a car accident. Is that righ
Ms. KAPTUR. Yes. He was
our State legislature the ne
or that weekend.
Mr. RUBIN. I am not famili
Ms. KAPTUR. You are not
A final question. If you a
in this Union right now, and
information about machines'
faced with is a barrage of p
you that their technology is
not be. Where do you go no
go to help you in your boar
thing about electronics, not
with this major public respo
tion? Where would you tell th

patch, which is something that changes certain parts of the software. It adds lines of source code or removes lines. And when you apply a patch, what you are doing is you are creating a new version of the software that is based on the old version but has certain changes. So a patch can completely change the behavior of a software package. It can make it better, it can make it worse.

And I also have read a lot about the patches in Georgia. I don't have any personal firsthand knowledge that anything like that happened. But I would say that it is a very, very serious matter that if a patch gets applied to a voting machine on Election Day or shortly before, that is no longer a certified machine; it's a different machine, and it needs to be recertified.

And so you need to be very careful. And this gets to the point that you mentioned about access between the election officials and the vendors. On Election Day, the vendors should not be tinkering with the machines and applying patches to them.

Ms. KAPTUR. Well, I will tell you, in the home precinct that I am from—and I'm a precinct committeewoman, long before I was a Congresswoman—they sent out an official from the company to deal with a scanner that was malfunctioning in that precinct, because we didn't have election workers that were trained to do that work. And I am thinking, what is going on here?

Mr. Chairman, I want to thank you for holding this hearing. I don't want to go overtime. I have two small questions I still want to ask, if you would be kind enough to——

Mr. PUTNAM. You have time coming.

Ms. KAPTUR. Do I have time coming?

I just wanted to ask you if any of you are familiar with the technology that Mr. Akin Gibbs had. He was one of the few minority contractors that had a technology out there that could have been reviewed by the States—they and localities—as they make selections. Do you know, is that technology still on the market and what its name is? He was in the State of Tennessee.

Mr. MORGANSTEIN. The True Vote?

Ms. KAPTUR. I think that was the name.

Mr. MORGANSTEIN. That is all I know about it. Sorry.

Mr. RUBIN. I had read accounts, I believe this person was killed in a car accident. Is that right?

Ms. KAPTUR. Yes. He was due to come to Ohio to testify before our State legislature the next week, and he died the prior Friday, or that weekend.

Mr. RUBIN. I am not familiar with his technology.

Ms. KAPTUR. You are not familiar with his technology. All right.

A final question. If you are a local election official in any State in this Union right now, and you are interested in getting accurate information about machines' verifiability and so forth, what you are faced with is a barrage of private companies coming to you, telling you that their technology is the best in the world. It may or may not be. Where do you go now for good information? Where do you go to help you in your board of elections? None of you know anything about electronics, nothing about computers. There you sit with this major public responsibility. Where do you go for information? Where would you tell them to go?

Mr. RUBIN. One of the things to keep in mind is that there are some questions that can tip off right away the kind of vendor you are dealing with. So, for example, Chairman DeForest Soaries of the Election Assistance Commission made a statement that election officials should have the right to ask the companies for their source code under nondisclosure to get external security reviews. The first question to ask a potential vendor is if they would be willing to do that, and, if not, why not?

And you could try to produce a list of questions—I have some actually on my Web site—that you might want to ask a vendor, just like you would when you are buying a car. If you start to see that they are acting shady, they don't want to answer certain questions, they won't provide you written documentation of certain things, then you would proceed with caution. I don't know if there is an independent group out there that is providing advice on vendors.

Mr. SHAMOS. There are no consumer reports for voting systems.

Ms. KAPTUR. And if I could just say for the record, Mr. Chairman, I thought when we voted for HAVA, that's what we were voting for. We were voting for the National Institutes of Standards and Technology to be the Fort Knox or the Oak Ridge or the whatever national renewable energy lab for voting, the place where you would go to get information.

Mr. SHAMOS. This should be the province of the Election Assistance Commission. Previously, it was the voluntary province of the Federal Election Commission, to accumulate information about voting systems. But they couldn't get into the position of making specific comments about particular vendors. It just didn't seem appropriate in that context.

Mr. PUTNAM. That would be contrary to Jeffersonian ideals, I believe.

Mr. SHAMOS. So the answer is now many studies are being undertaken by many organizations, and one must keep up with the output of these things to try to determine which are authoritative and which are not.

Ms. KAPTUR. I thank you for your forbearance, Mr. Chairman, Mr. Ranking Member. And we thank the witnesses very much for helping educate our whole country and many election officials who will watch this and are trying to make the best decisions they can at the local level under these circumstances.

Mr. PUTNAM. Thank you, Ms. Kaptur, Mr. Clay. Thank you very much for your input and helping us to get some good expert testimony. I want to thank all of our witnesses.

In the event that there may be additional questions we did not have time for today, the record will be open for 2 weeks for submitted questions and answers. Thank you all very much. This subcommittee stands adjourned.

Whereupon, at 12:34 p.m., the subcommittee was adjourned.]

○