UNITED STATES
FEDERAL COMMUNICATIONS COMMISSION

IN RE:)
)
CONTRABAND CELL PHONE USE IN)
PRISONS WORKSHOP/WEBINAR)

Pages: 1 through 94

Place: Washington, D.C.

Date: September 30, 2010

HERITAGE REPORTING CORPORATION

Official Reporters
1220 L Street, N.W., Suite 600
Washington, D.C. 20005-4018
(202) 628-4888
contracts@hrccourtreporters.com

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

IN RE:)
)
CONTRABAND CELL PHONE USE IN)
PRISONS WORKSHOP/WEBINAR)

FCC Building
445 12th Street, S.W.
Washington, D.C. 20554

Thursday,
September 30, 2010

The parties met, pursuant to the notice of the Commission, at 1:00 p.m.

APPEARANCES: JAMES ARDEN BARNETT, JR.,
Chief, Public Safety and Homeland
Security Bureau, FCC

ELLEN SCRIVNER
Deputy Director, NIJ

THOMAS KANE
Assistant Director, Information,
Policy & Public Affairs Division
Bureau of Prisons

PANEL ONE: JAMES ARDEN BARNETT, JR., Moderator
Chief, Public Safety and Homeland
Security Bureau, FCC

LAURENCE D. ATLAS, Panelist
Senior Advisor to Assistant Secretary
NTIA

COMMISSIONER CHRISTOPHER EPPS, Panelist
Mississippi Department of Corrections
Treasurer, ASCA

APPEARANCES: (Continuing)

JACK FOX, Panelist
Chief, Office of Secreity Techology
Federal Bureau of Prisons

CHRISTOPHER GUTTMAN-MCCABE, Panelist
Vice President of Regulatory Affairs at
CTIA

JULUIS KNAPP, Panelist
Engineering & Technology, FCC

SECRETARY GARY D. MAYNARD, Panelist
Maryland Department of Public Safety &
Correctional, Director,
Southern Region, ASCA

DR. NANCY MERRITT, Panelist
Senior Policy Advisor, NIJ

DR. JON OZMINT, Panelist
Director of the South Carolina
Department of Corrections, ASCA

P R O C E E D I N G S

(1:00 p.m.)

MR. BARNETT: Good morning. My name is Jamey Barnett, and I am the Chief of the FCC's Public Safety and Homeland Security Bureau -- and in California where I know we have some people joining us on the web. Whether you are here in person or virtually, via the web, thank you so much for attending and participating today in our workshop and webinar on combating contraband cell phone in prisons, jointly sponsored by the Department of Justice, National Institute of Justice or NIJ, the Association of State Corrections Administrators or ASCA, and the FCC.

I'd like to thank Pat Caruso, the president of ASCA, George Kemp, co-executive director of ASCA and Bob May, associate director of ASCA for ASCA's sponsorship and strong advocacy of solutions. I'd also want to thank Dr. Ellen Scrivner, Dr. Nancy Merritt and Joe -- of NIJ who have done so much to advance the discourse of solutions.

My name is Jamie Barnett and I'm the chief of the Public Safety and Homeland Security Bureau here at the Federal Communications Commission. Deadly serious, the crisis of contraband cell phones in

prisons is deadly serious. Deaths have occurred because of inmates contracting hits against witnesses, public safety and police officers, and others. They continue to run criminal enterprises.

This is why FCC Chairman Jankoski and the Commission have made finding technological solutions a top priority, solutions that are available immediately. The FCC has taken action. And the first of those technologies is now deployed because of that action.

Several weeks ago, I had the privilege of attending the launch of an innovative technology solution that we at the FCC called 'Inmate Call Capture' installed at the Mississippi State Penitentiary in Parchman, Mississippi. Commissioner Chris Epps of Mississippi Department of Corrections was kind enough to invite me, along with corrections officials from all over the United States.

Altogether about a hundred people were there on that bright, sunny day when we entered the 18,000 acre facility to see the first in the nation deployment of this new technology in a large-scale prison facility. And Chris Epps is going to be with us electronically today, but I'm going to steal a little bit of his thunder.

The demonstration was a huge success. Over 216,000 contraband cell call attempts were captured and kept from connecting in that first month along. State correction officials demonstrated how several call attempts by inmates, using cell phones with unauthorized numbers were blocked from ringing through their intended destination.

And in fact, my office couldn't reach me during that time because my cell phone was not registered. And when I tried to make a cell phone call, I got this nice little message from the Mississippi Department of Corrections that I was using an unauthorized cell phone. I did get to witness personally that that technology works.

We were joined in an effort by a large community of interest that includes state corrections departments, federal agencies such as the Department of Justice, NIJ, the Federal Bureau of Prisons, the Department of Commerce's NTIA, or National Telecommunication Information Administration, national organizations, including the American Correctional Association. I already mentioned ASCA, technology vendors and wireless carriers all exploring the most effective and precise technologies and the options that we can use to defeat cell phone use in prisons.

As a part of this effort we've consistently stressed the need to identify effective solutions to stop and prevent the illegal use of cell phones in prisons, which often serve as the vehicle for sustained illegal activity. The FCC's goal has been to identify those technologies that are lawful and address the particular challenge at issue, which would be available immediately or at least in the near future and without creating new problems. Today's workshop continues that effort.

Some of the topics that will be covered today in the workshop will include technologies currently available and that may, in fact, already be in use. We also look at legal constraints and policy concerns related to cell jamming and other interfering technologies. There are many intricate, interdependent issues that are involved, including the technical efficacy and adaptability, legal considerations, interference problems, preserving legitimate consumer and public safety and 911 wireless communications, the relative cost, which of course is an important part, including the impact on prison payphones, the land lines that they use and also avoiding unintended and harmful consequences.

To help us through these issues today, we've

gather what I feel is a distinguished panel of federal and state experts. We will open our workshop with some of their remarks, including our co-sponsors of the event, ASCA and NIJ.

ASCA provides essentially the viewpoint of the prison administrators and practitioners. And General Gary Maynard who has a tremendous record of service and is a retired general in the Oklahoma National Guard and he's a director of ASCA's southern region. He's here with us. And he, of course, is also the secretary of Maryland's Department of Public Safety and Correctional Services. And if you would raise your hand for those who can't see you.

Also representing ASCA today is John Ozmint, Director of the South Carolina Department of Corrections since 2003, graduate of the University of Alabama School of Law, former prosecutor and a commander in the Navy Reserve, which a Navy guy like me would like. Dr. Ozmint has been a leading proponent of the jamming solution and will be able to address that for us as well today.

I think that you will find that they will bring insights to us and we really do appreciate what ASCA has done to put these issues forward.

Our other co-sponsor, and also a great help

to us, is the National Institute of Justice. And we are privileged to have Dr. Ellen Scrivner with us today, Deputy Director of the National Institute of Justice and she will be making some opening remarks for us in just a moment as well.

NIJ has been a great partner of the FCC and has done much to bring clarity and focus to this issue, including hosting a number of meetings with a wide range of correctional experts and practitioners and as well as helping to establish a federal interagency working group tasked with identifying the necessary steps that the federal partners should take to find and advance workable solutions to this problem.

Also making opening remarks today at my left here, your right, is Larry Atlas, Senior Advisor to the Assistant Secretary of the National Telecommunications and Information Administration, hereafter referred to as NTIA.

NTIA has really conducted a number of tests of jamming devices in both the laboratory environment and at a commissioned federal prison facility in Cumberland, Maryland. We believe that these controlled tests produced results that have added to our understanding of jamming technology.

Further NTIA is charged by Congress, in coordination with the FCC and the Federal Bureau of Prisons with developing a plan to investigate and evaluate how wireless jamming, inmate cell capture, detection and other technologies might be used by law enforcement in correction applications in federal and state prison facilities.

Congress has asked that the plan consider the adverse effects these technologies may impose on commercial wireless and public safety communications services in areas surrounding prisons. NTIA has been working to develop that final report, and we appreciate the opportunity to have had input into this important document. And Larry, we appreciate you being here today.

Rounding out opening remarks is Tom Kane, the Assistant Director -- by the way, I did mean you all to be raising your hands. This is Larry. That's Dr. Scrivner. That's Tom Kane. He is the Assistant Director of Information, Policy, and Public Affairs Division at the Federal Bureau of Prisons. We've had the pleasure to meet with the Bureau of Prisons on a number of occasions and they bring tremendous expertise to addressing the problem of contraband cell phone use.

The Bureau of Prisons has spent over 10 years investigating technology to combat contraband cell phones and we welcome and look forward to hearing about BOP's experiences with various technologies.

Our experience to date has taught us that technology can provide a range of solutions. Our focus here at the Commission has been on the technologies that are not only lawful, but also specifically target the problem at hand without jeopardizing essential public safety, federal and state and law enforcement activities. Or quite frankly, the lawful use of cell phones by the public, including the ability to make 911 calls.

In order to better understand the technical aspects of the available technologies, Julie Knapp, sitting close to the center there, our chief of the FCC's Office of Engineering and Technology will walk us through these various technology choices that we have, following the opening remarks.

The central purpose of this workshop, however, is to initiate a free-flowing discussion of what has been accomplished to date, the lessons learned from trials, demonstrations and full scale installation of these technologies, and the directions we need to take and the obstacles to be overcome to

arrive at a range of workable solutions for prison administrators as they confront this challenge.

Therefore, we will spend a good time today in a Question & Answer session, featuring the return of Larry Atlas and General Maynard as well as some of the new faces that you see here, the representatives of the cellular industries and two states that have done so much in this area, Mississippi and Maryland.

In addition to General Maynard, we are pleased to have join with us on the phone bridge Commission Chris Epps of Mississippi Department of Correction, who like General Maynard is wearing two hats also representing ASCA since Commissioner Epps serves as treasurer of ASCA.

And we're fortunate to have Jack Fox, who is the Chief of the Office of Security Technology with the Bureau of Prisons. Christopher Guttman-McCabe, Vice President of the Regulatory Affairs with CTIA, the wireless association to provide the viewpoint of the cellular industry, our own Julie Knapp and last but definitely not least, Dr. Nancy Merritt of the National Institute of Justice who have been very close and abundantly helpful and a resourceful partner in this.

In order to facilitate certain technological

solutions, the commercial wireless providers have worked cooperatively with the FCC to develop regulatory steps, including executing spectrum leases where the necessary, and really they were all necessary to enable the operation of these systems as the inmate cell capture or call capture rather on their license spectrum. And I'm very pleased that with the carriers active support to enable testing and deployment of non-jamming technologies we were able to effectively work together for this goal. The carriers appear ready and we appreciate their participation in this.

Lastly, and importantly, I do encourage all those in attendance here as well as those logging in via Web-X to submit questions or observations you may want to have from the participants and panelists. Cannot promise that we'll have time to address all of the submissions, but this is an ongoing dialogue and your input has been and will continue to be a critical aspect of our efforts with finding solutions to this problem of contraband cell phones in prisons.

With that, I'm going to turn this over now to General Gary Maynard of Maryland for his opening remarks. And for those who are making remarks, if you could keep them around four minutes each. If you have

to go a over a little bit, there will be a small electrical shock in your seat. But other than that, I would turn it over to General Maynard.

GENERAL MAYNARD: I represent the Association of State Correctional Administrators today. ASCA is comprised of the 50 states corrections directors as well as the Bureau of Prisons and the Chicago, Philadelphia, and New York City jail.

The problem of illegal cell phones in the hands of inmates and prisoners is common among all these jurisdictions across the country. The possibility of illegal activity ranges from selling unmonitored phones to inmates to call their friends, through drug trafficking, extortion, gang violence to coordination of escapes, prison disturbances, and serious assaults on staff to the killing of witnesses in criminal cases.

We think that we should be equipped with all the tools available to control the illegal activity that cell phones allow. The range of options include the routine and random searching by correctional officers, cell phone sniffing dogs, detection technology, interdiction technology such as x-ray machines, walk-through metal detectors, embossed chairs to keep the phones out of the prisons, managed

access technology and jamming of cell phone signals.

We think there is no single solution. We think that corrections officials should be armed with all the options available in order that we can carry out our mission. And on behalf of the Association of State and Correction Administrators, we appreciate being invited today and look forward to the discussion. Thank you.

MR. BARNETT: Thank you, General.

As I mentioned earlier, John Ozmint is the Director of the South Carolina Department of Corrections. I failed to mention that he's also the chair of the Policy Resolution Legislation of Legal Issues Committee for ASCA. And I'll turn it over to you Director Ozmint.

MR. Ozmint: Thank you. I'm not going to restate the problem. Obviously, it's serious. I have probably have been one of the few at the table that had to go to the hospital and visit family and pray with the family when a staff member of ours was hit as a result of a cell phone -- of a hit put out by a cell phone. He miraculously survived. And so this has had a real impact in South Carolina.

And what I want to do is talk just a minute about that toolbox that we've al mentioned. We are,

by the way -- I'm not only here to speak about jamming and the fact that we think that tool ought to be in the toolbox, but we are also testing a managed access system in South Carolina. We have had tremendous cooperation from our wireless industry in our state. I think every carrier has signed up and volunteered to participate in that.

But I also want to remind -- I think my goal here is to remind everyone that we do want to have every tool in the toolbox. I look at this as a game of percentages. We've never asked to jam cell phones in the Baltimore City Jail. One, I don't own Baltimore. Two, I don't know that you can control signal strength jamming to the extent that you can do that.

However, I'm probably the only person at the table, with the exception of our friend from NTIA that has seen surgical jamming, directional jamming demonstrated. And I have, much as you did with, and I will soon do next week with our managed access test, I have turned on my cell phone in a building where jamming was taking place, walked right outside and turned it on and it worked. And I've seen dozens of people do the exact same thing, literally outside the walls of the building.

So what I think we need to talk about is where managed access is going to be the only solution. Obviously, I'm testing managed access in a prison where I think even in my system it's probably going to be the only solution. But in 80 percent of my prisons, they're sitting on 180, 200 acres of property right in the middle. And in those prisons managed access would be literally a waste of resources because there are no legal cell phone calls on prison property in South Carolina. None. There are no legal 911 calls. There are no legal calls home. There are no legal emergency calls because it is against the law.

So there are two types of legal -- that's what the concern is with any signal interference. And with regard to calls off of prison property, our set back lines in 80 percent of our prisons are such that we're not going to interfere with any legal signals off of prison property. But the only type of legal call is a legal call coming from prison property. But in my state there are no legal calls being made from prison property.

So if I'm not interfering with calls on the outside across my property line, then in those situations, those rural areas with long, large setback lines from other properties we believe jamming to be

the best solution.

In Maryland, that may be 20 percent of the prisons. In South Carolina, that may be 80 percent of the prisons. But we need to have every tool in the tool bag at our disposal. Thanks.

MR. BARNETT: Thank you, Direct Ozmint. And now I'd like to turn it over to Dr. Ellen Scrivner, Deputy Director of the National Institute of Justice.

MS. SCRIVNER: Thank you, Admiral and welcome to everyone.

I'd like to welcome you on behalf of Assistant Attorney General Lori Robinson of the Office of Justice Programs and our director, Dr. John Lobe, who is director as of about two months ago new to the National Institute of Justice and has had to testify on the Hill today or would have enjoyed being here himself to hear and participate in this discussion.

For those of you who are unfamiliar with the National Institute of Justice, our agency is really the research, development, and evaluation arm of the Department of Justice. And so what we support, primarily, is research that examines solutions to a wide variety of problems in the criminal justice system. And we are looking to provide objective, independent, evidence-based knowledge as well as tools

to meet the challenges of crime and justice, particularly at the state, local, and Tribal levels.

Our constituents tend to be at the state and local, Tribal practitioners and so we're very interested in conducting research or evaluating tools that will help people in those situations. And because of that we're driven by certain beliefs, and they're beliefs that are pretty typical of a research agency.

We believe that research can make a difference. In terms of the toolbox, we would want to see research done on all of those tools, sort of begin to evaluate those tools because we think research can help provide answers to many questions about individual lives and the health of communities, particularly the health of the correctional community.

And we also believe that our research agenda must be driven by professionals, by people like yourselves, those participating on the webinar in the real world. Those are the people who deal with these situations in crime and justice problems every day and so we need to hear from you in establishing our research agenda.

And our third belief is that partnerships with other agencies, with other government agencies

and professional associations are critical to determining what works. We could come up with a great agenda. We could come up with a research project. But if it didn't make any sense to you all, then we're kind of wasting everybody's time and money. So while much of our efforts go towards the funding of research initiatives, we are also very pleased, Admiral, to have the opportunity to really join with everyone here and to join with the field to really better understand both the challenges and the opportunities that are facing us in this area of the use of cell phones in correctional facilities.

Our intent as co-sponsors of this webinar is not to offer a solution to the problem or to take a position on a solution because right now we're the researchers we don't really know. But we understand it's there and we understand there may not be a single answer to the problem. But we hope that this webinar is going to really open the dialogue that helps us fulfill those research missions that I spoke about earlier. And a dialogue for an ongoing examination of the problem and its potential solutions from an operational, technical, and regulatory perspective.

I'm unable to stay for the entire webinar since this is a day of competing engagements. I have

another meeting on the other side of the city, but I'm going to leave you in very good hands with a number of professionals here who are actively addressing the issue at the state, local, and national level. And each will share their perspective on the problem and possible solutions.

But it's also geared, the webinar, to be a true opportunity for information sharing, that type of forum, and to give us the opportunity to hear from you as well. So please join the conversation by sharing your experience and your concerns with the group. The information you share will provide both panelists and the audience members with a more complete understanding of this issue and a range of interventions and options that are currently in operation or under development. With that, I will turn it back to the Admiral.

MR. BARNETT: Dr. Scrivner, thank you so much. We appreciate you being here.

I now turn it over to Thomas R. Kane, the Assistant Director of Information and Policy and Public Affairs Division for the Federal Bureau of Prisons.

MR. KANE: Thank you, Admiral.

I will not attempt to restate the problem

that Admiral Barnett and Secretary Maynard and Director Ozmint have described so well already. And I will agree right up front that I think the topic line of today's discussion for corrections should be -- I'll steal Director Ozmint's corrections need every tool available in the tool bag.

I will tell you a little bit about the Bureau of Prisons involvement in the review of these sorts of technologies and our perspectives on where we think we need to go next.

We have, as Admiral Barnett outlined, worked with NIJ for over 10 years to investigate technologies that detect or disrupt cell phone transmissions, yet we have found none that is both effective and affordable for corrections. And those are both key issues for discussion.

Given the difficulty of preventing the introduction of cell phones into prisons and jails, there is great interest in developing affordable cell phone jamming and managed access techniques in addition to detection. And we recognize there are some concerns about these technologies already alluded to by others. And we believe that additional testing and evaluation is necessary to access whether such technology will be effective in prison environments

comprised of high security structural features and in geographical areas where a considerable amount of legitimate cell phone traffic occurs adjacent to a prison.

We must confirm that jamming technology can be controlled precisely in well defined areas so that use in correction facilities does not interfere in the community with the communication of first responders or commercial users. And what we are not convinced of yet, Dr. Ozmint's comments notwithstanding, is what sort of configurations of jamming equipment would be required to work effectively in various architectural structures, especially in higher security facilities where we think structural challenges will be great, and developing and designing an effective solution in those kinds of situations could be very expensive.

We also must confirm that managed access systems in metropolitan areas do not interfere with communications of first responders and commercial users who are not registered with the managed access system.

We believe that the optimal solution may involve the use of jamming in some circumstances, managed access in other circumstances, complemented by detection technologies. Every tool available in the

tool bag.

We need to continue to look for cost effective solutions and work with others who can help solve the problem. Many of us here in this room need to partner. We want to continue building those partnerships to facilitate technology development and testing, including NIJ, NTIA, FCC, private vendors and other correctional systems. Our collective focus has the best chance of finding a reasonable solution.

We congratulate Maryland, Mississippi, and South Carolina departments of corrections as well as ASAC as an association, the FCC and NIJ for taking leadership roles in this area. We hope to have the opportunity in the Bureau of Prisons to evaluate jamming and managed access systems in BOP facilities, especially medium and high security BOP facilities for the reasons I mentioned a moment ago. And we will work with NTIA in considering how to evaluate the effectiveness of jamming and managed access solutions.

BOP appreciates the opportunity to participate in this webinar and we want to thank the FCC for hosting it and thank FCC, NIJ, and ASAC for co-sponsoring. Thank you, Admiral.

MR. BARNETT: Tom, thank you so much.

Laurence D. Atlas, as I mentioned earlier,

is the senior advisor to the Assistant Secretary of NTIA. Larry, thank you for being here.

MR. ATLAS: Thanks Admiral.

I thought when you're the last person to give the opening remarks the advantage is everything that really can and should be said has been said, so you can just reiterate a lot of it.

But I thought I'd give you a little summary of what we've been doing over the past year at NTIA related to this issue. NTIA is the President's principal advisor on telecommunications and information policy. And my boss, Larry Stricklin has spoken about this topic numerous times and I think there's a real clear consensus view in the Administration and clearly articulated that the use of cell phones by prisoners to carry out criminal enterprises is intolerable and demands effective technological solutions. And NTIA, the FCC, NIJ, the Bureau of Prisons over the past year we've all been working together to address this problem on a variety of fronts.

Late last year, we at NTIA in coordination with BOP conducted tests of cell phone jamming technology at the Bureau of Prisons facility in Cumberland. Prior to that test we did bench testing

of the equipment at our Institute of Telecommunications Services in Boulder, Colorado. We've issued technical reports. Two technical reports actually that detail those test results.

Congress has also directed NTIA to develop a plan to investigate technologies that might be used to defeat cell phone use by inmates and to report back to Congress. And in order to fully develop the record that would be used to create that report, in May we issued a notice of inquiry seeking comments on various technologies that have been mentioned here and that might be used to defeat contraband cell phone use.

We received a variety of very useful comments from manufacturers, from public safety and correctional officials and wireless service providers, and that report is now in the process of being written with input from our sister agencies as well.

We look forward to the continued collaboration with our federal agencies and state correctional officials to address a problem that we all agree is intolerable, but also very complicated. And it's complicated because we have to find solutions that are effective. That may be the easiest part. They also have to be affordable. And at the same time they have to protect legitimate use, not only by

federal users of the spectrum who are basically NTIA constituents, but also correctional officials and public safety officers themselves and the law-abiding public. Thanks for having us.

MR. BARNETT: Larry, thank you so much. There's a go-to guy at the Federal Communications Commission. That's Julian Knapp. He's our chief of the Office of Engineering Technology and he's going to provide for us really the technological or technical explanation of the available technologies. Julie, thank you.

MR. KNAPP: When Admiral Barnett asked me to provide a technical overview, he also mentioned do you think you can do it without the megahertz, the milvolts and the DBs. And that's hard for engineers to do. And so I just realized listening that my presentation is incomplete because I didn't include the cell-phone sniffing dogs. But hopefully, I've gotten at a very high level a technical overview of the technologies.

And for the engineers, I ask your indulgence for not making this very technical. One group you might call electronic sniffers. Sniffers effectively emit a low-power radio signal. It detects reflections from electronics. Not like a radar, but basically it

sends out a ping signal and it looks at a different frequency to see if there are electronics close by.

You've got to be close to the cell phone. I mean it can detect not only cell phones, but other electronic devices. But you've generally got to get close. And the one plus of them is that it will detect these kinds of electronic devices, whether they're on or off.

Second large group passive detection. Essentially, this listens for cell phone signals. It only detects the cell phone when it's active. It won't detect it when it's off. The calls could still be connected. You could do a few different ways. You can have a network of sensors that will triangulate the location of the cell phones and there are tradeoffs. The more units, the more sensors that you have the more accurate the location. There are also hand-held detectors that are available.

But in the end, it's just telling you there a cell phone there. Depending on the level of precision, you have to go out and locate it.

The next technology we'll talk about is jamming. Jamming is the deliberate radiation for the purpose of disrupting the use of electronic devices, equipment, or systems. Cell phone jammers are

frequency band specific. They transmit on the same radio frequencies as the cell phone and the idea is to over power the desired signals and disrupt the link between the cell phone and the tower.

They don't discriminate among cell phones within the range of the jamming signal. So that whether it's a contraband phone or a legitimate phone they're all disabled. Now what I tried to show in this diagram is it's very simple. We sometimes think of jammers as a single device. You can do it in different ways. You can use a number of lower-powered jammers that are strategically placed throughout the site to block the calls.

You can also do it by sending what engineers refer to as a leaky cable, a wire that emits the signal along the path. So you have to distribute the wire strategically throughout the area.

And the last technology that I'm going to talk about is what we've been calling inmate call capture technologies. It's effectively a mini cell site. The impermissible calls are not connected. The permissible calls are released from the mini cell and then connected to the commercial cellular network as usual. The policies for doing that are selectable by the system administrator. In other words, whoever has

set up that site. All of the 911 calls can still be connected.

So in 10 minutes or less I think we've touched on, again, at a high level the four main groups of technologies that we'll be talking about.

MR. BARNETT: We'll get somebody else, an expert on dogs if there are any questions on that.

So at this point then we'll move to our Questions & Answers. And I would encourage people on the web to put those in. We have a microphone here for the audience. Just to remind you here we have here. As I mentioned, Larry Atlas is at my left. Next to him, virtually, is Christopher Epps, Commission of Corrections for the Mississippi Department of Corrections. And I'm going to ask now. Chris, are you on the line with us?

MR. EPPS: I am and I'm here.

MR. BARNETT: Great. It's good to have you with us here today. And just so you know that when you speak we're going to flash a picture up here so people know who they're looking at. So we appreciate you being here with us here today.

Next to him, virtually, is Jack Fox with the Bureau of Prisons. He's the chief of the Office of Security Technology. Next to him Chris

Guttman-McCabe, Vice President of CTIA of the wireless industry. Julie Knapp, who you just speak. Secretary Gary Maynard of Maryland, Dr. Nancy Merritt of NIJ, Director John Ozmint of South Carolina. And then, of course, we have Tom Kane and Dr. Scrivner did have to leave.

So at this point, and since Commissioner Epps is just now joining us, if you could start off by just giving us a little bit of background of what lead to your decision and how you decided how to pay for it.

MR. EPPS: Okay. Thank you, Admiral. Let me say hello to everyone that's there.

What happened in Mississippi was real simple. We experienced from January 1, 2010, this year, until June 30th we found 1,994 cell phones in our prisons throughout the state of Mississippi. And we have known for three years we have had a problem. We have visited some of the solutions the gentleman before me described and we also were obviously concerned like everybody who is attending and listening today about public safety.

And I also have another factor that I'm concerned with and that is the cost -- the money that we're losing as it relates to our revenues that goes

to our inmate welfare fund for our inmates program. So that's what lead to the decision. We also have a state law that I'm not sure every state has that states that it's illegal to bring contraband into the facility. And in this state you can receive up to 15 years for such contraband.

We also search staff. We search inmates. We have dogs trained to find cell phone. In addition to that we prosecute staff and terminate them and we prosecute civilians. But after all of that we were still having problems with cell phones getting in through various means, and I won't get into those because most of you are already familiar with that.

But recently, we feel we have found a solution and we call it managed access. I heard the term used today captured access. And the bottom line, obviously, it allows us with the approval of our carriers at the Mississippi State Penitentiary at Parchman to block the signals, to capture the signal before it hits the tower of any call that's not authorized that's in the computer.

And Admiral, you alluded to it earlier, but from the 1st of August until August 28th, we blocked 216,320 calls. And we were able to do that -- just the other day the canine was performing a search and

the inmates had the cell phones on the writing table surface and one the canine said what is this. He said you can have it. It don't work anyway.

So we feel like this managed access is one way -- is one solution. And I'm proud of it. I've put in the policy here in Mississippi that effective October 1st and thereafter any inmate caught with a cell phone in the State of Mississippi will be transferred to Parchman.

We were able to get this system because somebody about now is wondering how much does it cost and how we were able to pay for it. It didn't cost our taxpayers at the Department of Correction one cent. We were able to get this system through negotiations with -- on an added value on our contract. They have to put in at our three largest prisons, being Parchman, Central Mississippi, and Green County. Those three prisons comprise of about 11,500 inmates. And so this will all be done before December 2011.

So Admiral, that's kind of a quick overview of, (1), way we did what we did, (2) how we were able to do it, and (3) we know that we are losing about $2 million of revenue with these cell phones because the average call in Mississippi is about $3.15 per call.

I turn it back over to you, sir.

MR. BARNETT: All right, Commissioner Epps thank you so much. And just to clarify for those who may not aware of the system. In essence, what you're saying is the inmate call capture was contracted through your landline for the prisoners. And then, in essence, the cost is passed on by those rates, is that right?

MR. EPPS: That's exactly right. I mean we all know that when an inmate has a cell phone obviously we can't record it. Obviously, we can't monitor. We don't know who they're calling. And so what happens is by them not using the landlines that we have done the best math we can and we feel like it's a couple million dollars. And those funds in my state, if I don't capture those, then I have to use taxpayer dollars to provide the teachers, the counselors, et cetera.

MR. BARNETT: All right, Commissioner Epps thank you and please jump in there. We can't see you raise your hand, so you have to be very forward on that.

Let me direct the question then to General Maynard. I know that you've been investigating this and leaning forward and looking at

a lot of different technologies. What would you say are the critical steps in evaluating this and what were the things that Maryland has used to try and decide the way forward? And maybe tell a little bit about what you're doing.

MR. MAYNARD: -- to see what technology is available throughout the country all the way from detection through jamming. So that should be on the street pretty soon. I have attended the demonstration at FCI, Cumberland, the jamming demonstration and we conducted some demonstrations in Maryland that included the managed access and detection technologies.

MR. BARNETT: Thank you so much. Let me open it up more generally now. And I would encourage the audience, both here and virtually, to get their questions into us.

Could you discuss for us just a little bit what the relative benefits and drawbacks of the various technologies are as you see them from where you come from?

MR. OZMINT: I'll address that. I think the first thing for those of us in corrections to do is to just make an admission. I guess I was the first director to say I got a problem. All the cell phone

detections, all the shakedowns, all the best efforts of our people, and we're pretty good at what we do, we were unable to keep cell phones from coming into our system.

If you're not familiar with the way prisons operate, especially -- it varies a little bit, depending on funding. But in the deep south, in South Carolina while it is staff intensive, we might have 35 people working a shift trying to watch 1800 inmates, trying to move them from one point to eat, to go to medical, to do what they need to do.

And so what cell phones enabled folks on the inside to do was to create a new pipeline for contraband. And the new pipeline for contraband in our state is simply throwing, shooting, dropping, flying, packages full of cell phones over the fence line. And because they're able to communicate with the person on the inside, the folks on the outside know exactly when and where to throw.

And if we intercept, and we have good intelligence right now that indicate we're getting about 75 percent of the phones coming in. And much like Chris, our system is a little smaller than Chris Epps from Mississippi, but we're seizing a thousand to two thousand cell phones a year. And that's probably

25 percent to a third of the phones that are being thrown over the fence lines.

So that's the problem. And we want you to understand while we recognize that all these other things that we can do internally are important and we're doing them. We wouldn't be here if we weren't admitting that we needed some help because the phones are going to make it in anyway and we can't find them all.

All right, once we get to that point, for us we recognize that each state is different. They're basically, as I identified earlier, there's two type of legal cell phone calls that we're worried about that either managed access technology or jamming technology -- there are two types of legal cell phone calls. Maybe before this discussion there was only, but now there are two.

There's the legal cell phone call that takes place off prison property. And in South Carolina and everywhere that legal cell phone call exists. That is a real problem. And so whatever technology you us it's going to give you a problem with that. We are testing managed access as we speak and our system is up and running.

And Chris gave some numbers. And the

preliminary numbers I'm seeing from the folks that are providing that for us are staggering, as staggering as the numbers you just heard from Director Epps. But that technology, too, if you deploy it in the Baltimore City Jail you're going to have some bleed issues. And it is incredibly precise. I've been amazed at how precise that management access antenna, that power level how precise they can be.

I was equally amazed with how precise the jamming technology that we saw demonstrated was. But with both of those in a certain percentage of prisons or jails in any given state you're going to have some issues that you're going to have to work through.

The other type of legal cell phone call exists -- and this is really important for everybody at the table to understand. In some states there's such a thing as a legal cell phone call made from prison property . I concede that. But in some states there is no such animal.

In my state there is no person who is authorized to bring a cell phone on prison property. It is contraband. It is against the law. It is the same penalty for bringing that on prison property as it would be if you brought drugs or a weapon on the prison property.

And so in our state we need not be concerned with the officer that I believe folks may be legitimately concerned about, but they are confused. We have plenty of mechanisms for our officers and our staff to be in contact in cases of emergency. We have a variety of methods and every prison system has those methods. So we address those methods of communication long before cell phones were even in existence and they've continued to today.

So the technology has to in some states recognize two types of legal cell phone calls. And in some states only one type of legal cell phone calls. But other technology, whether it's managed access or jamming, if you put it close enough -- if the property line abuts -- the walls of the institute abuts closely enough to a property line where you could make legal cell phone calls, then you're going to have some issues that you're going to have to work through.

Our request is simply this. Just with working through those issues with managed access right now as fast as we possibly can so we can get that system deployed where it needs to be, I think we need to be working through those issues with the other technologies that are available as well.

MR. BARNETT: So precision being a key

factor in what you're saying. Let me continue then with that theme of advantages and drawbacks. You mentioned getting close to the edge. What are the advantages and drawbacks and considerations from a technological or even a policy consideration.

MR. GUTTMAN-MCCABE: If I may.

MR. BARNETT: Chris?

MR. GUTTMAN-MACCABE: Larry talked earlier about the demonstration or the test that was out in Cumberland. And as we looked at the results of that that highlighted our concerns from the industry's perspective. This is I guess a quote from the NTIA report. 'For the outdoor locations were jamming was not intended, the results showed that jammer power was measurable at distances up to 127 meters from the building.'

So when we look at something like that where it was a confined test. It was not in a real-world environment and it certainly wasn't designed to jam the entirety of the facility. And yet, in that instance you saw up to 400 feet outside the intended area was jammed. And we obviously respect absolutely that this is a big problem that needs to be solved.

We do not have, as an industry, legitimate customers within the walls of prison. We're working

hard to find alternative solutions to try to capture this as evidenced by Commissioner Epps and the work that he and Governor Barbour did in Mississippi and Director Ozmint is doing in South Carolina. But we think that the solution to this problem can't create a follow on problem for legitimate users. I think that's been recognized here by everyone on the panel.

But our concern is that even with the best intentions and with the best testing, you can have a radio environment. Julius knows this better than anyone, but you can have a radio environment that will change from day to day. And we all know this because one day you'll walk outside your office and you'll have two bars and two minutes later you'll have five bars.

And the radio environment will change with the seasons. It'll change with the load on the network. It'll change with how the carrier's power up or power down their cell sites. And as I'm finding right now, it'll change as our carriers move from third to fourth generation technologies. And so with the best of intentions you install a jammer and it looks like it's working perfectly today and tomorrow and it's not.

And I have to say a lot of this gets pushed

back to the carriers, but there are a pretty significant contingent in the public safety arena who've also opposed jammers for similar reasons. And as you look at the intersection of commercial wireless use and public safety use and how there's some public safety use interleaved right now with commercial operations. And no matter what you think about the D Block proceeding at the FCC and where you come out, I think everyone understands that sometime in the next 10 years there'll be sharing of commercial networks and public safety networks.

And so, to us, we look at it as it's not just 911 calls. It's just legitimate calls. It's public safety operations. And we have yet to see anything that has been able to confine to a small measured area in the way of jammers. And we've seen some really terrible outcomes. I mean last month in Philadelphia was a perfect example where someone didn't realize they were illegally turning on a jammer, purposely turned one on and Center City Philadelphia went down for the better part of two days, including the GPS technology.

And so the Coast Guard was one of the first to realize that there was a problem as the manager of the GPS technologies. And then for the better part of

a day the FCC and some field office personnel and folks within government, the Coast Guard and others went out of their way to try to track this down. But you can imagine what had transpired in the interim when the system was down. And that's what we look at. We've got to solve this problem. Our carriers move as quickly as possible.

We had a call from Governor Sanford and Director Ozmint about three weeks ago to help them with their managed access program. Within three weeks, all of the large carriers have signed on and the fifth tier-two carrier has signed on. And just as quickly I know the FCC has gotten some grief for not moving quickly. I would completely disagree with that. At every turn they've moved as quickly as possible and this is a perfect example. Within three weeks, they had a STA granted out of Julie's shop to go ahead and do this.

So, to us, we understand the idea of every tool in the toolbox, and yet I have to say we are very, very, very afraid of one of those tools. It, by its nature, is designed to ruthless cut off service. And it does not stop no matter what anyone says. I mean here was the company that has been the poster child for we can have targeted. We can have strategic

jamming and they run a test, a very defined, a very controlled test in Maryland and it leaks beyond the walls. And that wasn't a full jamming demonstration. And that's where our fear -- our fear was confirmed with that test.

MR. BARNETT: Chris thank you. And I want to come back in a minute to the question of effect on public safety communications. But please, General Maynard.

MR. MAYNARD: I think part of my concern and our concern in the slow pace that things move. I mean this was a little over three years ago in Maryland that a witness in a murder trial was killed from a call and then more recently, what happened in South Carolina.

We can search. We can find. We can interdict. WE can keep phones out. But it only takes one call to get somebody killed. I was at the demonstration at FCI Cumberland and the results that I saw when I was there appeared to be more convincing than what you described.

As they described it to me, they were able to sort of modulate the frequency power to pull that in and stretch it out around the parameter of that facility. We started another frustration two years

ago, a year and a half ago. I testified before the Senate on the Safe Prisons Communications Act thinking that we would like to have the same authority in the states that the Bureau of Prisons have to at least petition the FCC, not get anything, just ask -- be able to ask. And that legislation would have made that possible, but I think that has died in the House and probably won't go anywhere. But that's a year and a half ago that we spent a lot of effort in trying to support that legislation.

And I think there are illegal jammers out there and that's what we don't want. We would like to follow the legitimate procedure to demonstrate because the only demonstration I've seen of jamming is what we saw at FCI Cumberland and I've seen a managed access demonstration there in Maryland. I think our industry, our people just need more opportunity to look at, ask questions, and explore all the avenues and all the opportunities that are out there as opposed to this very, very difficult and slow process to move through and be able to identify and look for our own selves.

Because as Director Ozmint mentioned, it's going to be a different -- I think the tool kit needs to have every option in it because I do have about

eight prisons and jail facilities in downtown Baltimore. They're just right on the sidewalks. I mean people walk by. They throw phones in. So you've got to have -- I don't think you can ever keep them out totally. So we've got to have some way to manage that and managed access may be a way. Jamming may be a way. But we'd just like the opportunity to explore all of those.

MR. BARNETT: Let me open it up to the whole panel then. We mentioned the downtown prison, so jamming can an inmate call capture in a dense populated area based on tests that have been done or other knowledge?

MR. OZMINT: I think that you're going to have a real problem with the walk-by phone users that are walking down a sidewalk or driving down a road that abuts directly up to that facility wall. I have to echo what Director Maynard said. We are pleased with the cooperation that we get from our carriers in South Carolina. Absolutely. They all came to the table. They have been good corporate citizens and they've opened up their bandwidth to us and our tests are going well. And I have no doubt it's going to be a success.

But our frustration has been if we're

testing this technology, why aren't we testing the other. Now I heard the worse case scenario I'm sure from my friend in the industry because I've talked to Mr. Largent about this too and I've heard the same numbers. So 147 meters. I have most of my prisons -- 147 meters, 400 some odd feet. I have most of my prisons are 400 meters from where a legal cell phone -- not the buildings that we would be jamming, but the fence line is 400 meters in any direction away from any place that is not my property. And therefore any place that you could make a legal phone call.

Admiral, we would love for your agency to authorize us to do a test so that industry doesn't have to worry about 147 meters. And we've got 15 or 16 prisons where that is exactly the case. And that's what I want people to focus on, not the exception to the rule, not one part of the problem, but the reality.

he prison that Captain Johnson was the intercepting cell phones. And the reason he was shot was because he was intercepting cell phones. He was doing his job. He was shot six times and left for dead. That prison -- I was going to bring a schematic of it. There's not a piece of property that I don't own within 400 yards of that fence line. So it is

very difficult to explain to Captain Johnson's family if the problem is 147 meters why we couldn't jam cell phones in the building where the hit came from that changed his life forever.

MR. BARNETT: That's a good question. I might also put that to Commission Chris Epps. Commissioner Epps, you've got a facility there that's 18,000 acres. I forgot how many inmates you have there, and perhaps you could tell us that. But how did you decide or what decisions did you make between pursuing jamming and pursuing the inmate call capture?

MR. EPPS: What happened Admiral was the reason we wanted to go with the call capture was we found that's the best (TAPE INTERFERENCE) not interfering with the 911 calls or the 611 calls or the lady that needs to make a call in an emergency. But Parchman is 18,000 acres. We even have staff that live on the grounds of the penitentiary. We lease out 8,000 of those acres. We farm the rest of it. So we have farmers on the ground.

But we've been able to work with our carriers, which AT&T Mobility, Team Mobile, Verison, and Cellular South to get their approval and we've been able to put our equipment on the water towers. And obviously, it's something that you have to

monitor, but everything is working well with this managed access.

MR. BARNETT: So your situation is not unlike Director Ozmint. What has been your assessment of jamming for your facility there?

MR. EPPS: One more time. I'm sorry.

MR. BARNETT: I'm sorry. Your facility in some ways is the same situation as Dr. Ozmint. What has been your assessment of jamming for your facility?

MR. EPPS: The problem that we encountered with jamming when we experienced and looked at that was blocking the signals for other individuals. Whereas, with these antennas and managed access, for example, we put some of those individuals who live on the grounds that have cell phones we put them in the system. The superintendent of the prison is in the system. Obviously, I'm in the system. Whereas, to my knowledge, the jammer that we visit on and studied, you didn't have those capabilities.

MR. BARNETT: Okay. All right.

I want to make sure I'm opening it up to the audience. You have a question here? If you would, identify yourself.

MR. BITNER: My name is Terry Bitner. I'm Director of Security Technology for ITT Corporation.

And we're the U.S. largest manufacturer of jamming equipment. And I guess I would just like to echo what CTIA is saying. We produce over a billion and a half dollars worth of equipment for the federal government every year in jamming. And we just don't believe that that particular technology can be controlled precisely enough, even to the 144 meter because there are too many environmental factors associated with that technology.

Our job is primarily forest protection today. And one of the problems we have, and we've solved, and it pains me not to want to sell the commander jamming equipment. But we, in theater, affected the GPS signal as well with jamming. And we were seeing UAVs being affected because the jammers earlier on until we were able to perfect that technology, which we have now.

So I personally think that we're headed down a dangerous path looking at jamming for that application. So that brings us back to two specific technologies. One which we built called detection and location. And I guess, Admiral, I'd direct this question to you.

I've listened to this discussion for six years now. I've been at it probably more than anybody

on the panel looking at this particular application. And what I see is we're trying to develop a threat picture. We're trying to protect inmates from inmates. We're trying to protect staff and we're trying to protect the general public.

Unfortunately, in Homeland Security you would never send a bomb squad out to disable a bomb and then leave the bomb beyond. And the problem is not the SIM card. It's not the RF transmission. It's the phone itself. The object is to capture the hardware and eliminate the hardware.

Once you've eliminated the hardware, it doesn't matter how many SIM cards you get into the prison, a SIM card is of no value to anybody. Only the hardware is valuable. And as these gentlemen know better than I, we've seen it in all the gang activities. The gang gets control of the hardware and allow others to get SIM cards. All of this stuff gets into the prisons, not by the fairy godmother. It gets carried in some way or thrown over the fence. And those are areas -- security is a multi-layered thing. You have to have a good front door. You've got to have a good staff. You've got to get a good setback. And you want to eliminate all these levels of contraband.

There's not a pointer that's going to point out there at drugs or at alcohol or pornography. But generally, what we've found when we use our system it acts like a compass. And so when you point to where the phones are at, when you go there you find other contraband. So we see that detection is not getting a fair shake in all of this just because people have to go do something. And my question is how many phones have actually been captured with managed access?

We've talked about what's been denied, but the hardware is out there. So what's here is what I'd like as a parting comment to make. Because we're part of intelligence and information warfare, the enemy always adapts. It adapts all the time. Every time you make a move, they make a counter move. Without getting the hardware out of there, when you pull out your blackberry or your smart phone, you have a memory card in there and a SIM card.

It is now just a very smart modality to pass unmonitored information. So instead of an RF link, you now have a sneaker net in and out of the facility. So all they're going to do if the phone is denied or if the phone is jam, what they're going to do is they're going to take the very same pictures. They're going to get their movies, all of their messages in

and out the same way they do today, but with the small, nine-gigabyte memory card that happens to be in this particular Verison blackberry.

So I would just challenge everyone to step back -- I'm not saying the one technology is better than another. But step back and look at the alternatives and options that are associated without removing the hardware. Thank you.

MR. BARNETT: So in essence, what are you saying, and I won't you to ask you to repeat your question. We've had a couple of references to toolboxes and so detection might be another one. So I'd open it up to the panel. Where is the detection? What have you seen?

Maybe Larry you could address this or NIJ or maybe our Federal Prisons folks. What have you looked at with regard to detection, or maybe I might even say advanced detection technologies?

MR. ATLAS: It's certainly something we will be looking at in the report. And Julius had on his slides mentioned it as one of the aspects of it. We do the same things that you do here, to some extent. While it does require us to go and take further action.

MR. OZMINT: We tested the detection. We

tested that system and it was great. When a phone went off, we knew it. And generally, 99 percent of the time we found it or we found parts. It's incredibly expensive. In fact, we couldn't even keep the one unit that we had in one building. And so hopefully the price will come down on that as part of the solution. But again, I don't think it's the entire solution.

MR. BARNETT: Let me turn it over to the Bureau of Prisons for just a second.

MR. FOX: At the Bureau of Prisons of the three technologies we're talking about we've not tested -- although we're interested in it or jamming. We have, however, tested the detection system. We have an active detection system at one of our penitentiaries right now. And in the very near future we're going to put another one in one of our medium security facilities in the South.

The detection system that we have in Atlanta, as Commissioner Ozmint said is very accurate. It pinpoints the cell phone. In fact, we're to the point now where we're adapting it to be able to be on a network where we can actually look at it, go scoop it up, and do that from across the country. The problem is, like most technologies, it is expensive.

MR. BARNETT: Yes, sir?

MR. PORTEL: I'm Bruce Portel with T-Core Networks. I want to agree with one thing that was just said is that you've got to get the hardware away from these guys. But our company, T-Core, provides managed access. And one of the problems that we see with detection jamming is that equipment has got to be close to, in close proximity to the inmates, to the guards. Managed access, our system at Parchman we have nothing in any of the cell blocks, in any of the fenced jailed areas. It's all away from everybody. It's totally secure. So that's what I see as a big thing. We're away from everything and we make those devices useless, basically.

I mean I think that's another challenge. That even though you may get jamming, but you've got to put those detectors in the buildings. You've got to put leaky coax in the facilities and they're going to get tampered with by inmates, by guards, by whoever.

MR. OZMINT: It sounds great. I wish it worked that way in prisons. It's like telling the military to find every EID. No, you turn the jammer on and you'll find the hardware.

MS. MERRITT: May I say something?

MR. BARNETT: Absolutely. Dr. Merritt?

MS. MERRITT: I do just want to jump into the toolbox bandwagon and mention that when we're talking about the toolbox we really have to be aware that it's not just the technology toolbox. Cell phones are contraband. If contraband is getting into the prison, so are other contraband. We need to find out how it's going in, what are the policies and procedures that are allowing it to get in. We need to look much more broadly.

It's more enjoyable to look at cool, new technology. But we also have to get down to the basics and look at what are the policies and procedures that are allowing this to happen. And one of the things that NIJ has been very interested in is getting a better picture of what is actually going on because we talk a lot about shootings and calls for hits and that type of thing. But it's primarily antidotal.

We need to really understand what is the prevalence of this problem and what's the nature of the problem because we can't get the proper solution until we know what the problem is. And the problem is going to vary. It's going to vary across different security levels, different types or architecture. So

when we're thinking about a toolbox, we really need to think broadly.

First, we have to know what's our problem and what kind of tools do we need. And then we have to think beyond technology. There are simple things, maybe not so simple, but more humanistic things that need to be dealt with as far as policy and procedure to determine how can we ameliorate this problem somewhat.

MR. GUTTMAN-MCCABE: Admiral, just one add on to that point. I think in addition to the technology one thing that we've pushed and supported is legislation. And I know that Director Ozmint and Commission Epps both have good, solid legislation in their states. Senator Feinstein put together a bill that made it a felony in the federal realm to possess a phone, any of the components of it, to provide it and it made it a felony.

And I think we've seen a number of states that have similar, not all states. I would push the states that don't have similar legislation in place to really do that because it is -- obviously, it's not the entirety of the problem, but it is helpful if states enforce provisions that make it a felony, and those that don't adopt provisions that make it a

felony so that you're beginning to impact the flow of these devices.

If someone makes $30,000 a year and can get a thousand for a phone, and the downside is that they may get terminated. And there are some states that you don't even get terminated if you get caught. Where is the balance? It's almost a non-decision for certain people. Whereas, if you're facing a year for each continuing element and a $5,000 fine and a year in a federal prison, I think that changes the dynamics of providing that phone a little bit.

Obviously, it's not the ultimate because we do have it in Mississippi and we do have it in South Carolina, but the goal is to tilt this enough that we begin to see some benefits.

MR. BARNETT: So Mike you're going to make your way to the thing. In the meantime, I'm going to ask one other question. We have one from the web right now. And I think I'm going to point this one toward Julie Knapp. Regarding the use of call capture method, what keeps the contraband cell phone from affiliating with the commercial site within range? In other words, what forces the cell phone to affiliate with the capture system instead of the commercial system?

MR. KNAPP: The way cell phones work is they keep tabs of the control channels of all the nearby base stations. So essentially, what happens is you make the cell site at the prison the loudest one. And so the cell phone is going to try to make it's call through the cell site at the prison. And it's only after that effectively it tries to connect. And let's say it's a call that should be permitted to go through. It essentially tells it, okay, go to a different control channel and connect through the network.

MR. BARNETT: Based on the comparison of approved numbers?

MR. KNAPP: Yes.

MR. BARNETT: Okay.

MR. MARCUS: At the risk of saying the obvious, virtually all the cell phones that are confiscated in prisons are anonymous, prepaid cell phones. The U.S. is one of the few industrial countries that allows the unlimited sell of anonymous, prepaid cell phones. And one of the major prepaid cell phone companies even gives you the option of making up a false name.

Most of the prepaid cell phone companies you have to give a name and address. It obviously can be

false, but one of the carriers facilities it by saying you don't want to give your name that's okay with us. So I think part of the problem is the glut of anonymous, prepaid cell phones that are out there, although just forbidding them is not the solution.

A second issue that I think the Commission should also consider, though, are the regulatory implications of managed access. Managed access has been successfully tested through the cooperation and leases as has been mentioned with the local cell phone companies. So far, that's been a success.

Prisons tend to be in remote areas. In remote areas the cell phone companies may well not be the four big carriers, may not even be CTIA members. In order for people's life and safety to depend on managed access to be working as part of the solution, there have to be guarantees that if a prison wants to go to managed access the local cell phone companies will cooperate. And I thin that needs a modicum of regulation to assure that that happens. It needs a modicum of regulation that they'll cooperate on reasonable terms.

I don't think the Commission wants to regulate that. But if the local cell phone company demands $5 million as a price to cooperate, there has

to be some sort of backup system.

And finally, not only does managed access have to work, it has to continue to work. And what differentiates the U.S. from other countries is U.S. carriers are not restricted to GSM and 3G. U.S. carriers have total technical flexibility and have since 1987. That's why Call Com started in this country and not in Europe because we gave people technical flexibility. It's been a great success. But there have to be guarantees that managed access will evolve with the evolution of the network.

And while conceptually there could be private contractual arrangements that say that, I think some modicum of regulatory oversight is needed and I would like to ask the panel specifically do they think that no regulation is needed or do they think that some small amount of regulatory intervention is needed to make managed access a full member of the toolbox, not just an option to be negotiated between the prison and the local cell phone companies?

I'm Mike Marcus. I'm a retired FCC employee and a consultant in spectrum policy.

MR. BARNETT: Thanks Mike. Let me open that up to the panel.

MR. GUTTMAN-MCCABE: I'll jump in since I'm

the regulatory guy. I'm not sure Mike meant this or not, but one thing I want to clear is a perception that there's a dollar transfer during this process.

First of all, the wireless carriers are not being reactive in this space. First of all, we've been proactive. We spent several days about eight months ago in CTIA's offices with our carriers and manufacturer members and had about eight or nine different technology companies come in, all of whom you've heard from today and including the one that is down with Commissioner Epps in South Carolina.

These are companies that we brought to the attention of the FCC and NTIA and Dr. Ozmint and Secretary Maynard and on and on. And the carriers were at the beginning of this and worked with these technology companies to make sure that their technology works in the prison environment. So the notion that this is companies coming to us and beginning a process I think is a little misplaced.

The notion that there's some form of carriers holding these vendors or the prisons hostage over dollars is also misplaced. In fact, as I said earlier, when Dr. Ozmint and the governor called about three weeks ago, and thank you. Mr. Ozmint has been very effusive in his praise, but the carriers did move

very quickly and they weren't all nationwide carriers. One is a regional carrier.

And at CTIA we've been very aggressive in making sure that our carriers, large and small, are aware of the need to work quickly with the technology vendors. And so from my perspective, the notion that regulation is needed is a little troubling because we've actually been at the forefront of this in advance of the federal government and arguable in advance of some of the corrections community, and we've lead a fair amount of the meetings. Secretary Maynard and I were on MPR about a year ago or so on this issue and we had already been waist deep in the issue by that point in time.

MR. BARNETT: Okay. Others on that topic? Yes, sir.

MR. WIENER: Jeff Wiener with Fabioni & Company. I'm wondering if the benefits of jammers haven't been overstated a bit. And I guess my concern is even if HR560 were to pass when Congress comes back November 15th we're still several years away from the FCC allowing state and local facilities to implement those jammers. And we've heard from numerous folks in the House that they have no interest in even seeing the legislation move.

We've heard from prosecutors who say I'm concerned about jammers. I'd like to be able to listen in on what those prisoners are saying on their cell phones and the managed access offers some of that. That we want to be here. We just don't want those phone calls fried.

The other thing is again I think they can be tampered with and I imagine the notion of creating a targeted jammer system therefore creates a very expensive system. And I don't know that everyone is factoring in that cost with the ability to target and keep it inside the walls. Thank you.

MR. BARNETT: All right. Yes, Tom?

MR. KANE: I'd like to respond to those points in part, but I'd also like to echo some of -- return to a couple of the prior comments made.

There have only been a handful of tests of jamming equipment in prison environments. The one in the Bureau of Prisons at Cumberland in cooperation with NTIA. We were proud to be involved in. But based on those handful of tests, I would say that the findings are neither dispositive or even generalizable.

And Dr. Ozmint's comment earlier that he has many locations that are sufficiently remote that

jamming is a strong feasible. We in the Bureau of Prisons have a majority of our prisons in such remote locations. And what I'd like to offer here is that, and at the risk of the loss of all humility I'm going to quote one of my opening comments. 'We believe,' the Bureau of Prisons, 'that the optimal solution may involve the use of jamming in some circumstances, managed access in others and detection to complement jamming and managed access.'

When we say all the tools in the toolbox, I think corrections has learned that we're not about to be given immediate authority to use technologies that we don't yet have authority for. What we're asking I believe today, thus my term 'may,' is that these are hypotheticals, including the comments being made from the perspective of one technology, vis-a-vis, another technology in a correctional setting.

In effect, we have to be very careful, I think, about generalizing from very limited circumstances, and even the Cumberland test was a very limited circumstance. Candidly, we had wanted to test that inside the secure facility on that site. And working with the vendor who was helping us set it up couldn't get it done in terms of the parameters that they had to face with respect to cost and the

extensiveness of the environment that was provided by the secure facility adjacent to where it was tested, which was the prison camp.

The point being, one that I also alluded to in the opening, and that is we need to look at other environments. Correctional facilities that are, as others have mentioned, high security, different security levels, older and newer architecture, how would you retrofit an older architectural circumstance and what would you more efficiently muse in a newly-constructed institution? These are all questions that I believe are on the table when it will come to at some later point a more advised, enlightened decision about what ought to be in the toolbox.

I don't think we're there yet. But what I'm really worried about is that we will cut off the opportunity to do the sort of testing we should do with the various options that exist before we decide that they're untenable, any of them.

MR. BARNETT: Anybody else on that point or the other comments?

MR. OZMINT: I have something. And it goes back to this issue of time. Gary mentioned it. We are frustrated. And it is true that a lot of

concessions were made with carriers who were involved in drafting the language of the Safe Prisons Communications Act. And so a lot of protections and it would take a lot of time, a great deal of time to get jamming deployed under the language that we worked out in good faith, at least when we were working on that language the carriers were in the room.

Here's my caution. And there is absolutely no question about it. More people will die if we take too long.

MR. BARNETT: I certainly understand that. So in the toolbox you would say we need to employ all of the things. There would be an initial thing of some type of capture that could be done in some places. Cost was brought up. Tom, you mentioned cost. Could you tell us a little bit about what you experienced? Or Larry what you all have seen. I don't know if you all looked at the cost questions with jamming. What are some of the costs limitations you've run into?

MR. ATLAS: I'll take some limited shot at that one. The parameters in the architecture of that test were largely a result of what the vendor decided they were going to put forward in terms of that system. The costs of that test were not paid for by

the Bureau of Prisons or by NTIA. So that drove it.

The other thing that I was very impressed with as a factual matter related to the test, and this came out in our report as well, is the degree to which both the field design of the test and the results are idiosyncratic. So it really drives up from an expense standpoint the deployment of these systems. And that's something I think we have to address overall because the biggest obstacle here for any of these systems is the degree to which the installation has to be customized across a variety of criteria.

And no matter what you put into the toolbox it doesn't do any good if it's too expensive for any of the prisons to use in a budget environment that is only going to get more challenging. And one thing that I was impressed with in the design of the test is how much work went into just the configuration of it.

MR. BARNETT: Continuing then with the cost, and I'll get to you next then. Commissioner Epps paid for his system, in essence, by rolling it into an RFP from their landline. And that's passed on, in essence, to the prisoners on a per minute fee. What would be the considerations, advantages, or disadvantages -- I guess maybe we see the advantage of the prison system doesn't have to pay for anything.

But what are the advantages and disadvantages of that?

Yes, General Maynard?

MR. MAYNARD: The procedure they went through in procurement in Mississippi may not be a procedure that's allowable in Maryland.

MR. OZMINT: There are tradeoffs with that. Our inmate phone calls are the lowest in the nation because we took all add-ons like that off. What happened was the general assembly took the profits away from us. So then we renegotiated a new contract and took profits away. So our inmates make calls to their families cheaper than anybody else in the country. We are pricing that right now for managed access.

The reality is right now I'm guessing jamming a little bit cheaper than managed access to deploy, based on the conversation -- I'm probably one of the few that's had a conversation with a jammer and managed access. But because managed access is going to get their first, their prices are probably going to go down. There's going to be competition in that marketplace. Jamming is going to give more competition in that marketplace. It's going to help us more be able to control that cost.

Right now the vendor that we're working

with, just to give you an idea bout scale, our average phone call is about $1.57 minutes for an inmate right now. That to put one managed access system in was going to drive that up to about a little over $3 and that was just one prison. That's why more tools are better than fewer. Just take the difference in systems. Chris has got 20,000 inmates, but he can cover half of his inmates with three systems.

I have 25,000 inmates. But I've got to cover roughly 16, probably 17 medium and maximum security prisons to address this problem. And every state is different. Some states have smaller prisons. Some states have larger prisons. And that is why it's so important. Having more options is going to be critical in terms of determining costs and also in terms of meeting the needs of all those thousands of different types of facilities.

MR. BARNETT: So different states have different regulations and then different prison setups.

MR. OZMINT: Yes.

MR. BARNETT: Yes, sir?

MALE AUDIENCE MEMBER ONE: I have a question that really follows up on just this line of discussion. And I've heard a number of proponents

inside the prison systems talk about the need for something now and how much it's going to cost.

And I know with regard to the role that my company made in the deployment that Chris Epps has down in Parchment those were particularly important concerns to us. We worked very hard proactively in less than a year to craft with the FCC, with the carrier a regulatory structure that would work that wouldn't be impeded by law or regulation so that we could put this system into place.

We worked proactively with Global Tel Link to come up with a solution where, and Chris Epps said himself this cost zero dollars to the taxpayers of Mississippi. I would just be curious to hear from any of the other technology solutions what they propose in terms of getting these regulatory legal roadblocks out of the way now, if there are any? And how are you going to get this thing paid for? I mean it's hard to compete with something that costs you nothing. Where's the money going to come from?

MR. BARNETT: Do the federal system, do you have the same situation where the inmates are charged for landline use?

MR. FOX: Our system is our inmates make local phone calls at 6 cents a minute and at 23 cents

a minute for long distance phone calls. And it's our intent, it's our goal to not pass this along to the families or the inmates themselves. And therein lies some of our concern with the prices.

MR. BARNETT: Chris?

MALE AUDIENCE MEMBER 2: -- from T-Core Networks. I would just like to ask the panel members to keep one thing in consideration as you look at all the different alternatives.

The number one thing I think I hear here is cost. And you can't look at just the initial cost. You need to look at the life cycle costs. And where the managed access solution we're software driven. We're not going to be changing our hardware. So once we basically get installed at a facility, most of our upgrades are software driven and it's not a forklift upgrade.

So I mean you really need to look at the life cycle costs. And I think were your initial observation is that you think managed access is a little bit more than jamming. I would tend to argue if you look at life cycle cost managed access is probably the cheapest alternative out there.

MR. BARNETT: Tom?

MR. KANE: I'd like to just offer one

additional comment with respect to how pay for these sorts of technologies. And I understand that some of the state legislatures may have a different view than the Congress will. But the Congress, of course, oversees us, the judiciary committees. And our interaction with those committees, and some members in particular who are powerful and who are not going to depart, I believe, any time soon tell us that it would be a non-starter for us, the Bureau of Prisons, to roll the cost of a new technology into the charges that we now levy against inmate phone calls, thus, Jack's comment earlier that our plan is not to do so.

And in fact, I think most of the people in the room are probably aware that Congress now is looking closely at the cost of landline costs or even VOIP calls for prisoners nationally. So I think while that may work in the short term at the federal level I'd be surprised if it ever would. And at the state level I think it's going to be problematic as time goes by.

MR. BARNETT: General Maynard, did you have something?

MR. MAYNARD: I actually have a question along with what Tom was saying.

A couple of years ago when we were looking

at demonstrating different technologies, back then in talking relative to jamming, relative to managed access, relative to just about anything everything was $250,000 per institution. I'm sure that has changed now. But I would be curious as to what Commissioner Epps, if he had to pay for it, what it would cost for Parchman, or Director Ozmint what that cost would be because as Tom is saying a lot of us when we -- we who grew up in the system saw inmate welfare funds from telephone calls being used for a lot of things. And our legislature found out about and they started taking the money from us. And it gets to be a balancing between how much do you charge these families of inmates and how much is the legislature going to allow you to keep to operate.

So I think the cost is significant and I think too everybody here comes from a different perspective. And there is no question that we in the business are concerned about staff safety and public safety and inmate safety. That's our primary driver and we have to operate within a fixed budget. We are doing, and I speak for myself and maybe John and Chris. We're doing everything we can to combat the illegal cell phones in the prisons without managed access technology and without jamming technology.

So it's not like we're sitting waiting to get the technology so we can sit back and take it easy and let it take care of itself. We are doing everything possible now. We just think these are two more options we need to look at.

MR. BARNETT: Yes, sir?

MR. MCNAMARA: Thank you. It's Gary McNamara and I come from a different side of the field here. I represent law enforcement. And I am a first responder. And as a chief of police from a municipality in Connecticut, I'm glad I'm here because I learn a lot. So if I'm not speaking as intellect to the topic as you all might. You might have been doing it longer.

But we entrust our directors, people in charge of prisons and in charge of law enforcement to address problems. We're problem solvers. Technology is a big problem. As a crisis negotiator several years ago, I had the unfortunate incident at a university trying to negotiate out 22 students who were held captive with an individual with an explosive device.

And very difficult the topic of technology and how -- that's a problem for us and we basically had no solution to it. But yet I'm entrusted to try

and solve the problem. The gentleman here in charge of the Bureaus of Prisons and the corrections departments are saying they have a problem. And they're looking for solutions. And one of them I mean as pretty clear as day is this jamming technology that apparently there's a large group of people that don't want that.

But my opinion, specifically with John's comments is he indicates it's a problem for him. He indicates that it won't affect anyone outside the prison. He indicates a willingness to try it and yet, we're debating that problem.

And to your point, dramatic as it may sound for those not in the business, it's true. This problem occurs 10 seconds ago. It occurs an hour from now. It's going to incur or occur until that problem is handled.

And I don't know why we're debating, and we have a lot of people offering different opinions. But from a problem solver opinion, you try it. And you say, you know what, that created one more problem, but let's back it down or address it a little different. Because we're out there every day our officers in New York, Pennsylvania, California are responding to instances where technology is creating problems for

us.

Now I know there's a debate on how we're going to handle that, but to Director Maynard's point of years and years and years. I think this committee will be in existence for the next 40 years talking about all the technology and changes because it's creating a lot of problems for us in the law enforcement side and in clearly in corrections.

So from my perspective, you have to look at the people that apply it. And the people that are applying it that are looking at the problem are saying that problem solution there is the one I need. I wouldn't see why we wouldn't say that's the way we have to go. And I understand there's some different opinions on that.

MR. OZMINT: And all we're asking to do is just test it. I've got one prison, by the way, it's a mile away from any property line. I own everything in a mile from the fence line. Now I guarantee you, you will not have any bleed out there. And let's test it. Let's see if it works. We're testing managed access. Our frustration has simply been over this question. Why are we not testing jamming?

MR. GUTTMAN-MCCABE: Maybe you're not aware of this, but the fact of the matter is it's currently

illegal. So there's a federal law preventing the use of these. So that's why we're having this discussion is there's a flat out law. And the reality is, and we've tried to walk this line where we know that the problem has to be solved. And hopefully, we can really drive some technology solutions. But there are a number of public safety groups that have opposed the use of jammers because of the concerns that it would bleed over into uses such as yours. That it would impact uses such as yours.

So some of the organizations have weighed in saying jammers are not the right solutions, but we do need to move quickly on the other alternatives.

MR. MCNAMARA: And I do appreciate that. And I know that we're working through some of those processes because they're problem for us too on the law enforcement side. There are places, however, that making a phone call from a cell phone is illegal.

MR. GUTTMAN-MCCABE: Certainly.

MR. MCNAMARA: It's illegal in his prison. That's an easy solution. If you can't make them, then you can't violate the law.

MR. GUTTMAN-MCCABE: I don't disagree. But if that were that black and white it would be a simple solution and we wouldn't be up here. The issue is

that -- I mean you have a vendor to your right who makes jammers who says he can't sell them to the people up here who say they have a problem. If that isn't a stare illustration of the concern, I don't know what is.

And they were in our office. They were one of the eight vendors that we had in there, showing their solution. But they weren't showing their jamming solution because they just don't believe it's the right solution.

MR. MCNAMARA: Sure.

MR. GUTTMAN-MCCABE: I mean the Canadian Mounties rolled up to a stoppage and there was a mobile jammer in it. There's a micro-level issue that we need to address. There's also a marco-level concern that if these devices get into the stream of commerce that you have people -- you have bad actors at a traffic stop deploying a jammer. And it doesn't stop, necessarily, with Director Ozmint and his facility that is a mile from any people.

What happens when there's an event and public safety gets deployed to his facility because he only has 30 or so employees there and all of a sudden public safety is in some way negatively impacted by the jammer?

MR. BARNETT: This might be a good segue because I brought up some of the quotes that some folks in the Bureau have pulled.

And so Julie, I might ask you first. You see the CIO in California and basically the 911 folks, the National Emergency Number Association and the Association of Public Safety Communications officials have expressed some concern about this. What could be the interaction between jammers and public safety communications?

MR. KNAPP: Sitting here as an engineer, and what's tough for me is that this sounds like a simple problem. It sounds like you just jam the cell phone. But cell phones today are smart. They operate in multiple frequency bands and they're going to be able to operate in more. And radio, we've been trying for years, doesn't quite follow man's laws. It follows physics laws. We can try and fine-tune it and so forth. And each band behaves differently.

So some of these bands are adjacent to public safety spectrum. So there are things you can do. I mean you can, for example, put in strong filters to reduce the energy. And some things are harder to do something about because the public safety radios inadvertently pick up some of that energy.

So the challenge here, as you go forward, is it's a much more complicated problem than just putting a single jammer on and that it will stop the phones. And I hear your point about test it and so forth. I think, as an engineer, if I was really trying to stop it that way how hard it would be to make sure that you don't have unintended consequences, which doesn't mean it can't be done. It just means it's really hard.

MR. GUTTMAN-MCCABE: And Julie, if I'm correct, is referencing stand alone public safety specific operations. The area where we have added on concern or further on concern is how many squad cars now are deploying to an area that actually have a Verison netbook or tough book, or an AT&T or a T-Mobile or Sprint?

And then, as we juts talked about, I know Julie and Jamie are in the heart of this. We've got a proceeding at the FCC specifically designed to integrate the usage of a commercial network and a public safety network. Unfortunately, we don't have interoperability with public safety community. How many times are they deploying to an event and using commercial devices to coordinate with one another?

So we look at this beyond just the potential for interference like 800 megahertz where there's

interleave to commercial operations and public safety operations. And we look at it to extend significantly to what is the future. And as Julie said, we're looking at a future with Wi-Fi and VOIP on our phones and so the technology has to be adept. It has to be nimble and it has to be able to move forward.

MR. BARNETT: We've got one other question that's come in from the web, and then I'll get to the folks that are the microphone.

I'm going to ask Julie to become a lawyer on this. How is Mississippi able to block cell phone signals? My understanding is that's not legally viable? Anybody else want to jump in on that? How is it legally able to block cell phone signals.

MR. KNAPP: I think legally these calls can't be made and connected. And that really is the simple legal answer from the engineering office.

MR. BARNETT: It's not blocking it. All right.

MR. KNAPP: Yes.

MR. BARNETT: Yes?

MALE AUDIENCE MEMBER THREE: Yes, we keep hearing about cost is the main deterrent to any of the tools that are available. And cost could be a deterrent to tools that become available in the

future. And as cost is the problem, people could be dying. And I think we're all wrapped around that we need to take some action now so that folks are dying. That we don't have more cases of the folks in Baltimore or more cases like the officer under your command in South Carolina that was attacked.

My thought is with a lot of folks on the panel that are a part of ACA and ASCA could there be an effort to go Commerce Justice Science, to the judiciary committees and say that -- and the folks on the panel who control burn grant dollars and the folks on the panel who control the OJP dollars that go back to the state and work in unison to create another pot of funds that is designed to go to the states to fund, whether it's managed access, whether it's dog, whether it's Mr. Bitner's technology to see if we can't build something like that into the budget in FY12 and FY13?

MR. OZMINT: I can speak for ASCA. We will be doing that. Each director in their states will be seeking that kind of funding. I think we're one step ahead of it. We want to know which technology best fits each one of our prisons and which technology is going to be the most affordable. And ultimately, we need to get there. Again, my point is we need to get there quickly, as quickly as we possibly can.

And yes, managed access is interference with a signal. It does stop the signal eventually, but it's not jamming. And so there are difference of opinions about whether or not the FCC has the authority to regulate in this area and at least allow testing.

MALE AUDIENCE MEMBER FOUR: Never having spent a day in law school let me point out that the industry viewpoint that the law does not permit FCC to authorize jamming is something that was challenged in a petition filed over a year ago by South Carolina Department of Corrections and 30 other states. And which raised the point that the legislative history of $ 333, which was not adopted in 1934, but was an 1990 amendment to criminalize certain jamming cases that previously weren't punishable under criminal law seems to have nothing to do with that.

And if the Commission were to look at the legislative history, it might decide otherwise. So we urge the Commission to put that petition out for public comment so the public has an opportunity to comment on that.

But furthermore, $333 is interesting because it doesn't say the FCC shall not authorize jamming. It says certain jamming is a criminal offense. And it

doesn't say it applies to FCC. It doesn't say it applies to NTIA. And a straightforward construction of the Communications Act would show that NTIA gets its power from $ 305 of the Communications Act, which specifically exempts it from 301 and 303, but does not exempt it from 333 or any other section of Title III.

So there is some legitimate questions. I understand the CTIA has that point of view and I understand there are various staff letters that have been sent out over the past several years that parenthetically have mentioned that interpretation of $ 333. But the people who normally sit on the podium up there have never had an opportunity to vote on what they think $333 means. And certainly, the courts have never spoken on what $ 333 means.

This application of 333 might be correct, but let me say it is not obvious when you look at the wording, you look at $ 305, you look at the legislative history the construction that FCC may not authorize jamming, but NTIA can is a non-obvious construct when you look at the way the law was written. And I think the Commission should review these legal details and decide on that.

And with respect to ITT and the jammers, I can only imagine a jammer the development of which was

paid for by DoD for a DoD problem might not be clean enough for this particular problem. That perhaps what DoD was interest in at the time. But that doesn't necessarily mean that someone given a clean sheet of paper can do that. NTIA's testing relied upon not their attempt to build the best jammer they could with off-the-shelf instruments. It relied upon building a device that charitably could be called -- it was marketed illegally in the United States. And one could imagine when you're selling a product illegally you don't put the best engineering resources into it.

So whatever results NTIA gets with their off-the-shelf camera it was not a device that was necessarily well engineered. So if you want to show that it caused interference, I suppose you probably could. But the question is a device which is engineered for the civilian use at hand, how well that does. That's an issue that remains to be seen. And I hope in our deliberations it is. It's not obvious to me as a techie that over jamming, both in terms of adjacent bands and hundreds of meters down the road is inevitable when good engineering is at work. Thank you.

MR. BARNETT: So I'm not positive I want to delve into a legal discussion or go through the

precedent, but Larry, legalities is that one of the things that NTIA looked at? Was it more a technical discussion?

MR. ATLAS: No, we didn't look at the legalities. I was a lawyer once. I was a lawyer once here and I enjoy not doing it. I will reiterate something that Mike Marcus said. We didn't manufacture the jammer. We didn't design the jammer. It was offered for tests. The vendor paid for the test, so it wasn't an endorsement of a particular product on our part. It was the one that was offered up and available.

MR. BARNETT: All right. Thank you.

MR. GUTTMAN-MCCABE: This is the same company that has said that the jammer was very targeted and able to be very much directed at a specific area and then confined to that area. And I think no matter how you interpret the tests and what you think about whether they're dispositive or not, the signals went significantly beyond the area that they said they were going to confine it to.

So this wasn't an off-the-shelf jammer made for anything. This was the company that's saying we have the technology to target. And if you read NTIA's report, it specifically says that the signals went

beyond the area.

MR. ATLAS: I think we should be clear about what the test was of and what it was not. The test was not designed to test -- it tested whether or not the jammer would (A) jam signals within the prison, and (B) whether it would interfere with, because we happen to know what they are, known federal operations in the area. It did not test, it was not intended to test whether or not there would be or was interference with cell phone calls outside the building in which the jammer was located. So that wasn't part of the definition of the test.

And just like Chris is here saying the signal bleed outside the prison, the governor of Maryland at the same time, right, was outside the prison, we were there, making a cell phone call. So all I'm saying is --

MR. GUTTMAN-MCCABE: But Larry.

MR. ATLAS: Please let me finish.

MR. GUTTMAN-MCCABE: Okay. Yes, sir.

MR. ATLAS: All I'm saying is both the call and the existence of the signal outside the prison are beside the point in the sense that it wasn't something that was part of the test. And it goes to what I think Tom Kane was saying was, look, all of these

technologies need a lot -- these weren't meant to be definitive tests and weren't. So did it move the ball down road? I don't think that they solved any of the issues really.

MR. GUTTMAN-MCCABE: It wasn't an indictment of the NTIA process. It was simply of the manufacturer has made claims that they can control the signal. And the governor was able to make a cell phone, but if I'm correct the jammer wasn't designed to jam anything but the federal signal. So just like the idea was the jamming technology only jammed the federal bands at the time, none of the commercial bands.

MR. BARNETT: Mr. Bitner?

MR. BITNER: I just wanted to go back to the cost issue again as it is associated with jamming.

We looked at what we would develop if we were developing a jamming system to do precision jamming. And I don't want to go into the bits and bytes and the DBs and multi-pathing discussion about why we would do it the way we would do. However, we would do it with a deployment very similar to detection, which would be an array of jammers that would be distributed. They way the law is written it says that the lowest minimum power you have to use to

jam.

So in order to do that, I'd have to distribute the power. The way to do that is with many antennas or transmitters, small transmitters around the facility. When we looked at that, what we realized that was if detection cost was a problem, you're really going to like the cost of distributed jamming.

And the point I'd like to make on cost associated with the three technologies detection is the only technology where you can grow it a little bit at a time. You can put in just a few sensors and figure out do I have a problem? Where is my problem? And then add sensors. Whereas, with jamming and managed access it's an all or nothing. So it has a very low entry cost. I mean we've got places in Virginia for $20,000 you can put a facility in. So I mean it's that kind of thing.

And Admiral, I don't want you to lose the original question about leaving the hardware behind because now it's an electronic reader.

MR. BARNETT: All right. Thanks. General Maynard, do you have something.

MR. MAYNARD: I just wanted to respond to the FCI Cumberland test. Governor O'Malley was there.

We were at the door of the facility. He had no signal. He walked 20 feet outside of the door, 30 feet and he called his mother back in Baltimore. So from a layperson standpoint, it appeared to me that inside that signal area there was no signals getting out. Outside of that, he was able to make a call.

MR. BARNETT: You'd mentioned your RFP earlier that it went from detection to jamming. Did that also include management access?

MR. MAYNARD: Yes.

MR. BARNETT: So is that something that you all are actively considering at this point?

MR. MAYNARD: Absolutely.

MR. BARNETT: All right.

MR. OZMINT: We tested on commercial bands. We had a letter from the previous chairman of the FCC and we ran a test in a single location, a single building and the equipment at that time -- we had a number of reporters in the room and we allowed them to bring their cell phones in for that test. And they would say we're going to let Cingular make a call. And the Cingular would be able to make a call, but I still couldn't on my Verison phone. And they did that several times.

And then they jammed the entire room and

then everybody was able to go outside and make calls. So again, all we're asking for is -- and that was an off-the-shelf jammer, I'm sure. Maybe it's something they sell overseas in France where they jam in prisons. I don't know. But I do know that it's almost like Columbus is saying the world is flat, but I'm not willing to prove it.

If the world's flat, let's get in your ship and let's prove it. Let's test it. Let's find out what we're capable of. Let's don't hide from a new technology that might very well be the answer in many places.

MR. BARNETT: I'll take one more, but it's got to be quick.

MR. FISHER: I'm John Fisher. I'm president of a company called Try Safety First. And what I'd like to talk about that I have not heard and I'd like to add to the toolbox is called protocol disablement. And I've put together a business plan that I would love to email everyone in here, if you provide me a business card, where I can outfit every prison in the country absolutely free.

I can also outfit every school. The cell phone is a major problem in schools. And what we'd like to do is use the phone as a teaching tool for

part of the class. And then when it's time to give a pop quiz, the teacher can flip a switch and all of the phones will go silent. And then we can also eliminated distracted driving within one meter of the driver's cell phone. And I can take care of all three of these. I can outfit every public transportation vehicle in the country, every school, and every prison absolutely free by my business model.

MR. BARNETT: I tell you what, I'm going to have to finish on this particular note. But I mean the other thing that I think is brought up is that more technologies will emerge. So I'd like to thank the panelist for your lively discussion, including Chris Epps who is not here with us physically, but really added to the -- and I would ask you now to join me in thanking our panelists.

(Applause.)

MR. BARNETT: To the National Institute of Justice, to ASAC we certainly appreciate the sponsorship, along with the FCC. I'd also like to thank Jeff Cohen in my bureau for his work on this, Tim May, Deborah Kline. I'm trying to look and see who else is over there, Deandrea, Deborah, Susan, all the folks who put this together. Thank you for joining us today. And thank you those out there on

the web for joining us as well.

(Whereupon, at 3:01 p.m., the meeting concluded.)

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

REPORTER'S CERTIFICATE

TITLE: Contraband Cell Phone Use in Prisons Workshop/Webinar

DATE: September 30, 2010

LOCATION: Washington, D.C.

I hereby certify that the proceedings and evidence are contained fully and accurately on the tapes and notes reported by me at the hearing in the above case before the United States Federal Communications Commission.

Date: September 30, 2010

Gabriel Gheorghiu
Official Reporter
Heritage Reporting Corporation
Suite 600
1220 L Street, N.W.
Washington, D.C. 20005-4018