Company: **FBI ACS ONLY ACCOUNT**

Conference Title: **Presidential Commission on Law Enforcement and the Administration of Justice**

Conference ID: **4278911**

Moderator: **Dennis Stoika**

Date: **April 15, 2020**

Operator: The following teleconference is recorded for Dennis Stoika with the FBI for the Presidential Commission on Law Enforcement and the Administration of Justice Teleconference on Wednesday, April 15, 2020 beginning at 3 pm Central Time, 4 pm Eastern Time. Good day and welcome to the Presidential Commission on Law Enforcement and the Administration of Justice conference call. Today's conference is being recorded. At this time I'd like to turn the call over to Director Phil Keith. Please go ahead, sir.

Phil Keith: Thank you Brandon. Good afternoon and thank you for joining us today. I'd like to call the President's Commission on Law Enforcement and the Administration of Justice to order. On behalf of Attorney General Barr, we thank you for joining us today for this important commission teleconference meeting.

As I mentioned yesterday this is our fourth week of teleconferences and we'll continue this process with three calls a week until the first week in June. We may have a break in May but we'll be sure to notify you of that. If the operating environment changes in a positive way, we could conduct a face to face commission meeting in Cleveland on the dates originally planned.

The Vice-Chair and I will do everything possible to keep you updated and informed of any changes that we see coming to the commission. At this time I'll request our Executive Director Dean Kueter to conduct a roll call of commissioners.

Dean Kueter: Great. Thank you Mr. Chairman and before we get started with the roll call, I'd just like to remind everyone, once again, this event is open to the press and for any members of the media on

our call. If you have questions or any clarification on anything, please contact Kristina Mastropasqua in the Justice Department's Public Affairs Office.

And with that Mr. Chairman, I will call the roll. Commissioner Bowdich.

Commissioner Bowdich: I'm here.

Dean Kueter: Commissioner Clemmons.

Commissioner Clemmons: I'm here.

Dean Kueter: Commissioner Evans.

Commissioner Evans: Here.

Dean Kueter: Commissioner Frazier.

Commissioner Frazier: Here.

Dean Kueter: Commissioner Gualtieri.

Commissioner Gualtieri: I'm here.

Dean Kueter: Commissioner Hawkins. Commissioner Lombardo.

Commissioner Lombardo: I'm here. Thank you.

Dean Kueter: Commissioner MacDonald.

Commissioner MacDonald: I'm here.

Dean Kueter: Commissioner Moody.

Commissioner Moody: I'm here.

Dean Kueter: Commissioner Parr.

Commissioner Parr: I'm here.

Dean Kueter: Commissioner Price.

Commissioner Price: Good afternoon. I'm here.

Dean Kueter: Commissioner Ramsey.

Commissioner Ramsey: Here.

Dean Kueter: Commissioner Rausch.

Commissioner Rausch: Here.

Dean Kueter: Commissioner Samaniego.

Commissioner Samaniego: I'm here.

Dean Kueter: Commissioner Smallwood. Vice Chair Sullivan.

Vice Chair Sullivan: Here.

Dean Kueter: And Commissioner Washington.

Commissioner Washington: Here.

Dean Kueter: Mr. Chairman, that concludes the roll call.

Phil Keith: Thank you. Are there any other announcements today?

Dean Kueter: No, sir, we're good to go.

Phil Keith: Thank you. Our focus this week continues to be on crime reduction. We want to discuss lawful access, the dark web, as well as contraband cell phones with security technology issues in jails and prisons. Lawful access is one of the top priorities of Attorney General Barr and last year the AG hosted a summit on this issue. Those of you not familiar with that summit, I encourage you to go the Department's website and search for the link for the summit. You'll gain greater insight into the many challenges and benefits of lawful access.

And to the Commissioners, we'll make sure to send you this information in our weekly summary. All Commissioners should have received the agenda and bios for this panel and we'll post the testimonies to the website as soon as we receive them. As we previously asked, we encourage Commissioners to take notes during the panel and we'll open for questions at the end of the testimony.

Now for part one of today's panel, we'll focus on lawful access and the dark web. We have Mr. Darrin Jones joining us who serves as the Assistant Executive Director in the Science and

Technology Branch of the FBI. He's also one of the Chairs of our technology working group. This is a side note. I was aware that Mr. Jones was recently promoted at the FBI. I know all the Commissioners join me in congratulating him on that magnificent achievement. Mr. Jones, thank you for joining us today. You're recognized.

Darrin Jones: Thank you Chairman Keith and good afternoon. Good afternoon Chairman Keith, Vice Chair Sullivan, Commissioners and guests. And thank you for inviting me to testify today. I've introduced - my name's Darrin Jones and I am the Executive Assistant Director for the Science and Technology Branch of the FBI. It is from within this branch that the FBI effectuates court orders for the interception of communications and assists our field office in accessing a wide range of digital evidence.

I've had a front row seat to view the steady erosion of law enforcement's ability to access electronic evidence and conduct court ordered - court authorized electronic surveillance. Over the last decade a number of U.S. major corporations have chosen to independently design and implement certain forms of technology, in this case increasingly complex user controlled encryption, offensively that no one other than the users can readily or timely access the contents of communications or other stored data.

As is well known, this results in the creation of lawless spaces on the internet where law enforcement even armed with a constitutionally sound search warrant or wiretap order are incapable of readily penetrating. These lawless spaces represent an ever expanding universe of illegal and illicit activity which threatens the lives and safety of our children, our economy, our national security and even our elections.

As was mentioned, in addition to my position at the FBI, I also currently serve as the co-chair of the Commission's technology working group. On behalf of that working group I would offer the following recommendation. Federal legislation must be enacted to compel major technology companies to

design for themselves strong encryption regimes for their products and services that protect privacy but that permit lawful access pursuant to the due process of law. Now that language may sound familiar to many of you. The working group decided to mirror the language adopted by resolution in December of 2019 by more than 30,000 members of the International Association of the Chiefs of Police representing over 160 countries around the globe.

For more than 200 years our Constitution, the Fourth Amendment and our courts have balanced our privacy and the need for law enforcement to have access to evidence society needs to stop criminals, pursue justice for victims, and protect its citizens. Why should it be different in the digital world? We now find ourselves in a place where not the courts but individual companies are deciding what's of greatest importance for all of us. Put another way, we're allowing technology to dictate our national core values rather than ensuring our national core values drive how we implement technology.

It has now been 131 days since a foreign terrorist in Pensacola, Florida murdered in cold blood three U.S. service members on a U.S. military base. And before being killed in a shootout with law enforcement the terrorist took the time to put a bullet in his cell phone in a clear attempt to destroy it and the evidence it contains. We are still trying to access that phone. That's what I mean when I say we have a lawful access problem.

In a recent gang task force case, source reporting and traditional telephony intercepts indicated that the main subject, suspected of ordering the homicide of another drug dealer, was using FaceTime to discuss and coordinate criminal activity with his co-conspirators. Indeed, he frequently directed them to use FaceTime instead of traditional cellular telephones because FaceTime, a product designed and implemented by Apple, employs end-to-end encryption. Post-arrest statements by the subject confirmed they were all well aware that those **not** arrested were only those co-conspirators exclusively using encrypted communications. That's what I mean when I say we have a lawful access problem. In a recent OCDETF investigation, indications were that multiple

subjects were responsible for illicitly transporting large quantities of heroin, methamphetamine, cocaine and marijuana from the southern border to the Great Lakes region regularly used encrypted apps to evade law enforcement detection. Senior members of the drug trafficking organization routinely instructed underlings to use WhatsApp, Telegram or Snapchat. Communications that would go unanswered on traditional cellular telephones were immediately accepted and responded to using encrypted apps.

As most of you are aware, Mr. Zuckerberg has announced that he intends to encrypt Facebook Messenger soon. What that means is, one man has independently decided to implement technology, in this case end to end encryption, in such a way that even if a judge issues a warrant, no one, including law enforcement can access those messages. In 2019 Facebook's platforms, primarily Facebook Messenger sent over 15 million tips to the National Center for Mission and Exploited Children. NCMEC immediately forwarded those tips to state and local law enforcement across this country. They took them to judges who issued warrants which allowed those agencies to rescue thousands of kids. One man, one company is independently deciding whether or not that should continue.

The ubiquity of end-to-end encryption and other user-only encryption products and applications causes them to be encountered nearly daily by state and local police departments. The impact of this challenge not only means an increase in unsolvable crimes and a denial of justice for victims but also manages to dramatically alter the nation's dual-sovereign federal system of law enforcement. Now let me explain that.

When local police departments are without resources to timely and cost effectively gain lawful access to encrypted evidence, they will necessarily have to turn to larger federal agencies, such as the FBI for assistance. Under such a paradigm the foreseeable result may be that federal agencies may reluctantly, but practically, find themselves in a position of effectively dictating which

state and local crimes are investigate and prosecuted regardless of the priorities of state and local officials.

State and local agencies must maintain lawful access to electronic evidence in order to retain their basic jurisdictional sovereignty and to ensure that enforcement of local crimes is controlled at the local level. The impact and magnitude of the lawful access crisis in the United States has grown to a point where the public safety trade-off to the citizens of this country can and should no longer be made privately and independently in the corporate boardrooms of tech companies.

It must instead be returned to the halls of the people's democratically elected and publicly accountable representatives. Ladies and gentlemen, let me be very clear. The FBI supports the use of strong encryption. It is critical to ensuring our infrastructure and our online privacy. But we absolutely believe that strong encryption models can be implemented by these companies in a way that is in accord with long time accepted Constitutional theories of privacy and civil liberties, continues to support robust cyber security, and provides for court ordered lawful access.

Thank you again for the opportunity to address this commission and I look forward to your questions.

Phil Keith: Thank you Director Jones for your most informative testimony. And again, congratulations on your new role at the FBI and your service to our country.

Darrin Jones: Thank you sir.

Phil Keith: Our next panelist is Mr. Cyrus R. Vance Jr. who is the District Attorney of New York County, New York. District Attorney Vance has been in his role for more than a decade. Mr. Vance, we thank you for joining us today. You're now recognized.

Cyrus Roberts Vance Jr.: Thank you and good afternoon Chairman Keith, Vice Chairman Sullivan and the Commissioners of the President's Commission on Law Enforcement and the Administration of Justice. On behalf of my office and speaking on behalf of our partners, particularly in state and local law enforcement, I want to thank and commend this commission for holding today's virtual panel on technology issues encountered by law enforcement.

And I want to thank you for the opportunity to testify on lawful access and encryption, an issue that is definitely vital to national public safety but equally vital and critical to safety in local and state jurisdictions. This past December I testified before the United States Senate Judiciary Committee on the urgent need for federal legislation ensuring lawful access.

Based on this testimony, my office subsequently met with senior staff from Google and Apple in February of this year to discuss potential ways forward and possible solutions. Unfortunately as a result of that meeting no substantive changes have resulted. And like the former speaker, I am convinced that federal legislation is required to achieve lawful access.

When I think about tech issues faced by law enforcement, to me the single most important challenge in the decade that I've been District Attorney, is the expanded use of mobile devices by criminals to plan, execute, and communicate about crimes. Just as ordinary citizens everywhere rely on digital communications, so do the people involved in terrorism, cyber fraud, murder, rape, robbery and child sexual assault.

Now, until the fall of 2014, Apple and Google routinely provided law enforcement access to their mobile phones when they received a court-ordered search warrant. But that changed when they rolled out their first mobile operating systems that, by design, often make the content of smart phones completely inaccessible. And in doing so, and very importantly, Apple and Google effectively upended centuries of American jurisprudence holding that nobody's property is beyond the reach of a court-ordered search warrant.

Our most recent internal data from our fifth annual report on smart phone encryption and public safety puts the growing problem in sharp belief. And I'd like to direct the Commissioners' attention, if they have our draft written testimony, to page four of our written report. And when you look at that graph, you can understand that our office receives in our own cyber lab in criminal investigations on average 1600 mobile devices each year, with almost half of those being Apple devices.

. Now the percentage of locked Apple devices has increased substantially over the five years from 60% in 2014 to more than 82% in 2019. So that means for Apple devices alone we receive over 600 locked and encrypted devices each year into our lab. Second, I'd like to direct the Commissioners to page five of our report and the pie chart that illustrates that more than 50% of the mobile devices that we received last year were connected to investigations into serious crimes, crimes of violence, such as homicide, sex crimes and assaults.

So, how has this affected law enforcement and crime victims? I'd like to answer those questions with two brief examples from my home office. The first involve child sexual abuse. There was a babysitter at a local church in Manhattan, who was identified as having shared images of child sexual assault online. Pursuant to a search warrant issued by a judge his encrypted mobile phone and other devices were seized.

Now over time we used - over time we opened the devices using technology from a paid consultant, and we then discovered, once we had the devices opened, the suspect was not only sharing images of child sexual assault, but sexually assaulting other children, and recording that abuse as well. Based on this evidence, access to the device, we convicted him of predatory sexual assault.

In the second example we were not so lucky. My office was investigating a case of sex trafficking and obtained an encrypted phone from a suspect who had been incarcerated on a different case.

In a recorded telephone call of the defendant in prison, the defendant told an accomplice that he hoped his phone had the newest encrypted operating system.

And the inmate is quoted on the prison recording devices as saying to his associate on the outside, and I'm quoting, "Apple and Google came out with this software that can no longer be unencrypted by the police. If our phones are running on IOS 8 software they can't open my phone. That may be a gift from God". In fact, we were never able to view the contents from this man's phone and as a result our investigation of sex trafficking was blocked by encryption.

Now to be clear, we are in some cases able to gain entry into these phone by using hacking tools we pay private companies to obtain. However such third-party workarounds are cost prohibitive for all but a handful of local law enforcement agencies, as the previous speaker referenced. Those costs are simply out of reach for many of our nation's smaller rural communities. In addition, these workarounds in many cases do not succeed due to security mechanisms put in place by Apple and Google.

It's also important to note that in most cases the ability to open phones and access them has led to the exoneration of people wrongly suspected or arrested for crimes so our ability to access devices enables us to protect our two-fold obligations, to hold the guilty responsible and to protect the innocent.

Finally, if Apple were participating in today's panel. Its representatives would likely tell you it's impossible for the company to open its devices without creating a hole for crypto-criminals themselves to gain access, and I have two responses to this. First, in 2016 Apple's then General Counsel acknowledged that the company's process for unlocking phones in response to warrants prior to 2014 had never led to a security breach.

Second, this new criminal justice problem is the direct result of these private companies' decisions to re-engineer their products. I'm not a technologist but I'm confident the problem could be solved by a company redesign as well. As President Kennedy once said, our problems are man-made. Therefore they can be solved by man.

To that end, I would offer three recommendations to this commission. First, that federal legislation is necessary for law enforcement to break the encryption stalemate that prevents us from obtaining evidence subject to a court ordered search warrant from a smartphone and social media giants. If they made a business decision valuing privacy, above public safety, I believe it's imperative that Congress acts to protect our citizens.

Second, the commission should urge tech companies and law enforcement to meet on a regular basis to discuss lawful access and define paths forward. Third, while the entire lawful access ecosystem, including ‘data in motion’ must be addressed, restoring lawful access to ‘data at rest’. That is ‘data at rest’ on the smartphone devices themselves. We believe it is an achievable solution, near term, that would help local law enforcement with the challenges we face.

Thank you again for inviting me to testify and for your efforts on this important issue.

Phil Keith: Thank you District Attorney Vance for that important testimony and thank you for your service. Our next panelist is Mr. Chuck Cohen who's the Vice President of the National White Collar Crime Center, also known as NW3C. Mr. Cohen brings a wealth of experience to NW3C as a retired Indiana State police captain. Mr. Cohen, we thank you for joining us today. You're recognized.

Chuck Cohen: Mr. Chairman and Commissioners, thank you for allowing me to testify this afternoon on the very important topic of dark web child exploitation and human trafficking. For background, I recently retired from the Indiana State police. Among my responsibilities was serving for 14 years as the Indiana Crimes Against Children Task Force Commander.

I'm currently the Vice President at NW3C, the National Crime Center, which provides training and technical assistance for state and local police, prosecutors and other criminal justice professionals. And I'm a professor of practice at Indiana University Bloomington, Department of Criminal Justice. I need to preface my testimony by saying that technology is neutral. It's not good or bad. It doesn't cause people to commit crimes or not commit crimes. It's just technology.

But what is true is criminals tend to be early adopters of emerging technology and to subvert emerging technology to facilitate and obfuscate the criminal activities. And this is especially true for online child sexual exploitation and online sex trafficking. I also must tell you that I hate the term dark web. I used it in written testimony and I'll use it in this testimony simply because it is commonly used by others. I dislike it for several reasons.

Among those, it is commonly misused. I also dislike the term dark web because it makes the technology sound scary and spooky. It's not scary and spooky. Much technology was originally created by the U.S government for very important purposes. But the unintended consequence is what people call the dark web, as it has evolved and continues to evolve into what amounts to lawless spaces where criminals can victimize children, communicate with each other to normalize their offenses against children, and work together to hone the trade craft of the victimization.

And for a variety of reasons that I tried to outline in my written testimony, we see a rapid evolution towards what was once the surface web becoming just one more area of the dark web. State, local, territorial and tribal law enforcement routinely encounters offenders using these networks and technologies to conceal and obfuscate their identities and locations during the exploitation and abusing of children.

What I've seen over the preceding decade is a systemic and seismic closure of avenues that are available to police for the identification and location of victims and offenders and the collection of

evidence in forensically sound manners when investigating these types of child victimization. In my written testimony I made four very specific recommendations that can help police protect children and interdict these type of offenders.

First, there needs to be increased funding for and availability of consistent and high quality training and technical assistance on a large scale for state, local, territorial and tribal law enforcement related to all issues outlined in this testimony. With increasing frequency during the normal course of business, state, local, territorial and tribal law enforcement inadvertently encounters the sexual exploitation and trafficking of children in which various aspects of dark web technologies are being used.

Also state and local law enforcement now routinely encounters dark web technologies in the course of conducting investigations specifically focused on the sexual exploitation and trafficking of children. My second recommendation is the implementation of regulations and laws that require internet service providers and companies providing commercial VPN or virtual private networking services to retain certain records and certain record retention or record retention periods.

A model for this is the Bank Secrecy Act or BSA and subsequent anti-money laundering legislation which set record retention and retention period requirements for financial institutions. BSA and subsequent legislation was enacted in recognition that through no fault of financial institutions. They were routinely used by offenders to conceal proceeds of unlawful activity and launder money.

In much the same way VPN and service providers are used to conceal and obfuscate the sexual abuse and trafficking of children. My third recommendation is an update to the Communications for Assistance to Law Enforcement Act also known as CALEA to require the internet service providers to provide assistance to law enforcement similar to that which CALEA currently requires for landline and cellular carriers, because they increasingly provide similar services to landline and cellular carriers.

This includes such assistance for law enforcement when the communication is encrypted. I've heard two major objections to such an update. First that this would simply push offenders to encrypted communication platforms and those located outside the United States. We have several years of evidence that this would not occur.

WhatsApp implemented default ubiquitous end-to-end encryption in April 2016. And there are numerous companies located outside the United States that offer end-to-end encrypted communication. Nonetheless, the National Center for Mission and Exploited Children estimates that in 2018 Facebook submitted nearly 12 million cyber tips related to child exploitation and child sex trafficking specifically associated with Facebook Messenger.

Offenders gravitate to, and will seek out platforms, where their intended victims spend time. The second argument I hear is that there is a binary choice between security that encryption provides, and lawful access to evidence such that we must make a hard choice between one or the other. It is noteworthy that both CDMA and GSM cellular protocols are encrypted and widely understood to be secure for users.

Nonetheless cellular carriers are compliant with CALEA in providing investigative assistance to law enforcement. The fourth and last recommendation is to make a resource that provides current and correct contact information for apps offered in the Apple App Store and Google Play Store readily available to law enforcement.

This can be accomplished through a requirement that Apple and Google maintain and make available to law enforcement such information for all apps available in the United States version of the App Store and Play Store. Offenders routinely use communication, image hosting, video sharing, file hosting, gaming, dating and social media apps to exploit and traffic children.

With one million iOS apps available in the Apple App Store and 2.8 million Android operating system apps available in the Google Play Store, it is often not possible for law enforcement to identify or locate the person, people or business that created the app or might retain information associated with the use of the app.

This leaves law enforcement with no one to whom an emergency disclosure request can be made or on whom legal process can be served. The two entities with the ability to collect the contact information and make it available to law enforcement if needed in the course of a criminal investigation involving child exploitation or human trafficking are Apple and Google.

Again, thank you for inviting me to testify and for undertaking this critically important work being done by the commission.

Phil Keith: Thank you Mr. Cohen for your informative testimony and for your service. Our next two panelists will focus on contraband cellphones and other security technology issues in jails and prisons. The first panelist will be Director Bryan Stirling. He is the Director of the South Carolina Department of Corrections. Director Stirling, thank you for joining us today and you are recognized.

Bryan Sterling: Yes sir. Thank you very much. This is Bryan Stirling, Director of the South Carolina Department of Corrections. I want to thank the President, Chairman Keith, Vice Chairman Sullivan, our working group on cellphones, AG Barr. I especially want to thank Beth Williams and her team at DOJ. They've been particularly helpful on this matter.

When I first took over at the Department of Corrections on October 1, 2013, I learned of a case where a correctional officer, Captain Robert Johnson, who was a contraband confiscator at Lee Correctional, was targeted and shot in his house five or six times point blank because he was doing his job at Lee Correctional to find contraband cell phones.

The hit was ordered from a prison, that same prison, via a contraband illegal cellphone. It was such a sophisticated plot to kill him that they used a .38 so there would be no shell casings left. What folks need to know on this call and in public, is that inmates are physically taken out of society by going to prison; however, they are virtually out there amongst us still committing crimes. You can look no further than the crimes and indictments that I've included with - on the back page, back two or three pages of my testimony.

We're asking for a couple of things today. We're asking for a federal communication interpretation of the Communications Act of 1934 that was updated in 1990 which says that states cannot block - or it says authorize calls or cannot be jammed. The federal government can jam calls but the states cannot. We don't think that Congress contemplated the fact that prisoners making calls from prison to commit crimes were authorized calls.

As a matter of fact, in preparing for this, I had pulled a report from that the Senate Committee on Commerce, Science and Transportation from back in November 19, 1989 and looked specifically at this language and it was not contemplated that states could not block cell phones, therefore protecting citizens from people that have been sentenced and committed to prison.

We would like, secondly, congressional hearings to get the industry on the record, just like a grand jury, so we know exactly what their technology is. We know if they can geo-fenfe our prisons to make it safe, because right now it's just not. These cell phones are everywhere inside our institutions.

Support statutory changes. I know Senator Graham, Senator Cotton, Congressman Kustoff introduced legislation that would allow states to jam just like the federal prisons are allowed to jam. Third, we're - or fourth, we're asking for creation of a pilot project that would allow jamming in four states so we could evaluate jamming.

Last year I was given special authority as a special US Marshal to conduct, along with the Department of Justice and others, a jamming test at one of our institutions. It was the first one where we actually had inmates in a dorm, and you will hear a lot about bleed over and 911 calls.

I can tell you that I was on the phone with my head of security. He was out of state at that time. And I was on the phone with him and we had it set up so we could jam inside the facility, inside one dorm, and I was talking to him and I said, "I'm stepping in." And when I stepped into that door, my phone immediately cut off. I was one foot outside that door and my phone worked and one foot inside the door, my phone stopped working.

So I think the red herring that the industry is presenting on jamming is just, with the way technology has gone, is no longer a problem, and it can be micro-jammed, as they say.

The last thing we would like to see is potentially a change in the law that would allow, which was in the Senate version, and it didn't make it into the House version, therefore it did not make it into the updated act in November 19, 1989. It was Section 334 which said that the FCC or federal or state authorities could turn off or ask for an order to turn off cell phones.

Right now this is called - the FCC has proposed to use the stolen cell phone database. Well they've said to us and others that what we need to do is get our states to change the law so that we can go in and get an order to give it to the cell phone companies to turn off these phones. Well that's going to be 50 laws in 50 states which will take a long time to do.

At the very least we would like the House and the Senate to look at potentially allowing state prisons to use IMSI-catchers to identify the phones that are illegally being used inside our facilities, turn that list over to a federal court and have the federal court order the industry to shut those cell phones down. State by state is just not going to work.

Thank you for your time on this and I'm happy to answer questions. Again, this is a - just a vital public safety matter. We see officers being hurt getting these phones or trying to take these phones from the inmates. We see drug rings. We see murders. We see child pornography. We see gang activity. We've seen fights inside our prisons. There's nothing that I've not seen on the street that I don't see on these cell phones that's happening in prisons. Thank you, Mr. Chairman. I appreciate your time.

Phil Keith: Thank you, Director Stirling, for your informative testimony and thank you for your service.

Our final panelist of the day is Chief Todd Craig, who's the chief of the Office of Security Technology for the Federal Bureau of Prisons. Chief Craig, thank you for joining us today and you're recognized.

Chief Todd Craig: Good afternoon, Chairman Keith, Vice Chairman Sullivan, commissioners and distinguished colleagues. Thank you for the opportunity to address the commission and present our perspective from the Bureau of Prisons.

I've seen firsthand the danger of contraband cell phones as warden, associate warden and chief of security technology. I've chased contraband cell phones in our prisons in snowstorms, desert and heat across the country. Criminals do not stop being criminals when they are incarcerated. They use these devices to facilitate illicit activity, including possessing and distributing child pornography, drug trafficking, gang activity and on and on.

Two promising technologies, managed access systems and micro-jamming solutions, are currently being tested in the field; however, additional funding and authorities are required to make these technologies available for broad deployment by both the Bureau of Prisons and state correctional systems.

Contraband devices get into prison a number of ways, inside people and objects, thrown over fences, increasingly drones are used to drop them into our facilities, and compromised staff. We deployed a number of other securities technologies to interdict cell phones, whole-body imaging devices, sophisticated walk-through metal detectors, thermal fencing, K9 units and fixed sensor and handheld radio frequency detection.

However, as Director Stirling indicated, there are always issues with staff safety when they're physically locating and removing these contraband devices. There are numerous factual situations detailed in my written testimony that point out the need to pursue contraband cell phones in prison as a matter of public safety, and I appreciate the work of the commission in this regard.

In Puerto Rico in February 2013, an 11-year veteran and investigator with the Bureau of Prisons was executed going home from work after nine inmates conspired and used contraband cell phones to orchestrate that murder. I was on the security assessment team that went in after that horrific incident.

To put things in perspective currently, last year we recovered more than 8,000 contraband devices and brought to prosecutors, U.S. Attorney's Offices, over 700 cases for potential prosecution. This year, there've been over 1,000 phones recovered from both secure and non-secure facilities. Ten cases out of 87 referrals have been accepted by the U.S. Attorney's Offices for prosecution.

The two technologies I referenced currently being tested in corrections are managed access and micro-jamming. Managed access is a distributed system of radio frequency antennas that capture all cellular signals, allowing known signals to go through, called white-listing, and blocking others.

The system captures all cellular signals within the geospatial confines of the prison - not outside, not in the communit -, within the geospatial confines of the prison, and disables unauthorized

signals from reaching the network. It can also be configured to provide intelligence for internal prison security and future criminal prosecution.

Micro-jamming solutions emit a signal that is stronger than the signal from cell phone towers outside the prison, preventing cell phones from being used within the institution. It jams all cellular signals within the geospatial confines of the prison, does not interfere with signals outside the perimeter and - but does not provide intelligence for internal prison security.

What is the Bureau of Prisons doing in regards to these two technologies? Last year we conducted ten mobile managed access assessments, targeting institutions with significant numbers of seized phones. This technology is portable and can be relocated and is the basis for either searching and finding the device or potentially getting a court order.

We know this technology works. At FCI Berlin, for example, last year our technology identified five contraband devices by identifying data, the IMEI and the IMSI, and the staff subsequently recovered those same five devices. Micro-jamming tests in January 2018, in collaboration with the National Telecommunications Information Administration, Department of Justice, Office of Legal Policy and others, we conducted a micro-jamming test of one device and one cell at our institution in Cumberland, Maryland. It was successful.

As Director Stirling referenced, in April of last year, we, in concert with South Carolina Department of Corrections, tested micro-jamming in one housing unit and it was successful. We did observe cell signals inside the housing unit were blocked, text messages, data connections, everything, but calls outside the one-foot perimeter of the exterior of the inmate housing unit could be made. So these are promising test results.

In this fiscal year, once we get through the current COVID crisis, we do plan to deploy a pilot for an entire institution for micro-jamming and a pilot for an entire institution of managed access, as well

as conducting 25 additional mobile managed access assessments to locate these devices. This will provide a comparison of these interdiction technologies and a sound roadmap going forward for the Bureau to interdict contraband cell phones.

We continue to work with federal and state partners to find ways to interdict these phones. Federal agencies are permitted to jam at federal institutions with NTIA approval. However, state and local facilities, which house the vast majority of our country's inmates, are regulated by the FCC and current FCC interpretation of law prevents state and local facilities from jamming signals.

Prosecution. In 2010 the Contraband Cell Phone Act was passed for federal prisons. It modified the Federal Prison Contraband statute, 18 USC 1791, and added an additional one-year penalty for possession of a contraband cell phone. We're working with the department to increase that to a felony five year penalty.

There's increasing synergy of technologies used by associated of inmates to circumvent our institution's security, namely drones and contraband cell phones. We've had a number of incidents, including one last month at the Federal Corrections Institution, Fort Dix, New Jersey, where a drone was identified flying over the institution. An inmate was subsequently apprehended with 34 phones, headsets, chargers and SD cards. It is an ongoing criminal investigation.

In closing, contraband cell phones are a significant security challenge to our prison system. While not often fully appreciated by the public, contraband cell phones can result in ongoing criminal enterprise, injury and even death to both our staff and inmates. It is a constantly evolving challenge and threat. What can the commission do?

We respectfully recommend that the commission ask NTIA and FCC to support spectrum use requests from correctional agencies to deploy micro-jamming, managed access and mobile managed access interdiction technologies, recommend that federal, state and local legislators fund

these contraband cellular interdiction technologies, including micro-jamming, as a matter of public safety, as well as statutory changes to effectuate deployment of those technologies.

Finally, recommend the wireless industry cooperate with corrections and law enforcement in developing low-cost, innovative wireless interdiction technologies to ultimately remove the threat of contraband cell phones from the over 7,000 federal, state and local jails and prisons across this country. Thank you for the opportunity to share my testimony. Thank you for the critical work that the commission is doing and for considering these recommendations.

Phil Keith: Thank you, Chief Craig, for your valued testimony and your service. Commissioners we will now open for questions. Just as a reminder, commissioners with a question are requested to state your name prior to your question and direct the question to a specific panelist that you have a question for, or if it's for a response from the entire panel, please state so. Just as a reminder to commissioners, your mics are hot at all times. Thank you. Commissioners with questions?

Commissioner Evans: Chairman Keith, this is Commissioner Evans with a question, if available for District Attorney Vance.

Phil Keith: Yes, sir. You're recognized.

Commissioner Evans: Thank you. District Attorney Vance, first of all appreciate your testimony today, and your time coming forward to the commission. You had mentioned in your statement that you'd met with some elected officials regarding lawful access and can you give the commission any insight on the barriers that those you met with might have moving forward on lawful access legislation? I think that's something that might provide the commission with some clarity on how recommendations could be framed. I'm interested to get your thoughts on that process.

Cyrus Roberts Vance Jr.: Thank you, Commissioner Evans. I have met with innumerable elected leaders over the course of five years since this began in 2014 when Apple and Google changed their devices to be full device default encrypted. So I've met with members of Congress, testified before House committees and testified probably two times before Senate committees.

I will say this: I hope I'm being responsive to your question. In our discussions with elected leaders in 2014 and 2015, I feel there was a couple of things that weren't happening. Number one, the administration, at that time the Obama administration, was not itself prepared to put forth a legislative solution that it would support, and consequently I think that acted as a reality that made it more difficult for elected federal representatives to come up with their own solution, because they were unsure whether it would be supported by the president.

When I testified this last December before the Senate Judiciary Committee, I found a completely different audience, to be honest. While I wouldn't say every committee member that was there, they were certainly 85 to 90% were, and I think with one exception, the senators, Democratic and Republican, looked at this issue differently, perhaps because over the last several years we've seen that the very companies that are claiming privacy and anonymity really is what should be guaranteed when they buy these devices.

The senators were aware that enormous cost came from that, and in addition of course those companies, while touting privacy, were also mining their customers' private information and marketing it to third parties for billions of dollars a year. So, Mr. Evans, I think that the bloom is off the rose of the tech companies that was on the rose in 2014.

I think there is a better understanding of the serious nature of the crimes that are used on mobile devices and using encrypted technology and that, quite frankly, the Senate Judiciary Committee said to us, myself and tech representatives there testifying, either figure this out or we're going to

do it for you. So I think there's a greater appetite to take stronger and more concrete measures to achieve a federal solution, commissioner.

Commissioner Evans: Thank you.

Commissioner Rausch: This is David Rausch.

Phil Keith: Commissioner Rausch, you're recognized.

Commissioner Rausch: Thank you. One is to the folks on the whole legal access piece. I appreciate their testimony and the effort. It's absolutely critical and we continue to push this message and we have conversations, I think the district attorney there, where he's right on target with the appetite I think in D.C. now.

Our senator, one of our senators here from Tennessee, has been helping us in leading the charge to push for, you know, basically what we're saying is, let's have law enforcement even in the technology world able to do our jobs. And that's all we're asking, and I think that point is getting across that there shouldn't be any aspect of our society where policing can't take place and that's what was being created and what they're trying to create. And so thanks for that testimony from each of you all and we'll continue to push that.

And on the cell phone issue in our prisons, I think that's another critical safety issue. We're seeing it. We just had a major, and still working a major drug case that is international and all being run out of a nearby state prison and by a gang. And it's literally, they're working an international drug trade, the largest that we've ever seen and we've started obviously making inroads in that and making arrests, but it's certainly a major issue.

I do have a question for those - for the chief and for the director. On the jamming, just to help me understand, if the jamming takes place inside the facility, what would the impact to your staffs, your COs there be in terms of their ability to communicate? Will there be an impact and how, you know, how would you all work the issue there?

Bryan Stirling: No impact. Nobody's allowed to take - well there's a limited number of people that can take cell phones in. It'd be the warden and maybe one other person. We would use our radios to communicate, just as we do now.

Chief Todd Craig: Same for the bureau, yes. We know government phones are no longer allowed in our facilities and the micro-jamming technology does not impact the spectrum, for example, where our Motorola radios are used.

Commissioner Rausch: Thanks. I know that that's occasionally brought up as a reason why not, but I appreciate you all verbalizing that. Thanks.

Phil Keith: Other commissioners with questions? Other commissioners with questions?

Operator: As a reminder, your lines are open. Please be sure to unmute your phone when asking your question.

Phil Keith: Thank you, Brandon. Hearing no questions, let me close by thanking our panelists once again for your time and your most valuable testimony. The responses to the questions from commissioners were well received. On behalf of the attorney general and his leadership staff, Rachel Bissex, Jeff Favitta and all the commissioners, your contributions provided today are most sincerely appreciate and will assist the commission in their deliberations and work.

Before we end the call today, just a reminder to the commissioners. Our last call for this week is tomorrow, Thursday April 16 from 2 to 3 pm. We'll be hearing from panelists regarding strategies and practices for law enforcement and technology use in crime reduction.

Are there any questions or comments from commissioners? There being no further business before us today, the President's Commission is adjourned. Thank you again, commissioners, for your dedication and commitment. Please be safe.

Male: Thank you, Phil, appreciate you.

Male: Thanks, Phil.

Phil Keith: Thank you all.

Male: Thank you, Phil, and bye-bye.

Operator: This concludes today's call. Thank you for your participation and you may now disconnect.