

President's Commission on Law Enforcement and the Administration of Justice

HEARING FIVE (Days 4-6)

REDUCTION OF CRIME

April 14 – April 16, 2020

Summary

Call to Order and Welcome

Chair Phil Keith welcomed the attendees to the fifth hearing of the President's Commission on Law Enforcement and the Administration of Justice. On behalf of Attorney General Barr and his leadership team, Chair Keith expressed appreciation for everyone's ability to attend the hearing. Chair Keith greeted and thanked everyone for attending and supporting the teleconference.

Opening Statements by Commissioners

Chair Keith opened by explaining that the three days of hearings, April 14 through April 16, would focus on crime reduction, including domestic violence and sexual assault; technology issues encountered by law enforcement; and leveraging technology to reduce crime. The first day's hearing focused on Domestic Violence and Sexual Assault. Witnesses for the hearing included Matthew Gamette, Laboratory System Director, Idaho State Police; Ms. Kim Garrett, CEO of Palomar, Oklahoma City's Family Justice Center; Richard Hertel, Prosecutor for Ripley County, IN; and Robert Hawkins, Chief of Police, Muscogee Creek Nation.

Note: Prior to the hearing, panelist biographies and written testimonies were delivered to the Commissioners for their consideration and review.

The Dilemma

"I've chased contraband cell phones in our prisons in snowstorms, deserts and half across the country. Criminals do not stop being criminals when they are incarcerated."

Chief Todd Craig



Domestic Violence and Sexual Assault Panel, April 14, 2020

First Panelist: Matthew Gamette, Laboratory System Director for the Idaho State Police Forensic Services and Chair for the Consortium of Forensic Science Organizations

Highlights:

- Law enforcement investigators need more access to forensic labs and disciplines because they are losing the ability to perform trace analysis due to the expense and training required for investigators, so courts do not have that evidence to consider.
- More must be done at the federal level to support the practice of forensic science by bolstering foundational or applied research and efficient ways to implement validated technologies in the laboratory and to facilitate technology transfer.
- Scientists must work collaboratively with law enforcement for the successful and quality application of field instrumentation by police for drug detection, DNA, and breath alcohol.
- Controlling DNA processing backlogs requires more scientists, bigger facilities, and funding. Controlling backlogs also requires controlling intake. It is important then to meet in triage teams with the labs, investigators, and prosecutors participating collaboratively in the evidence selection process.
- Labs need to know when cases are no longer being investigated or prosecuted so they can stop work on one case and move onto the next critical case. The lab should not be the arbiter of the law when determining rape kit components or which rape kits are tested. This can potentially violate either state or federal statutes: there should be national standards.
- For productivity and speed, labs are processing kits for DNA in an assembly-line format, while outsourcing kits to private labs and limiting the number of samples tested per kit.
- Forensics labs have an incredible amount of actionable and time-relative data that is not being leveraged to predict emerging drug threats, gun crime, and DUI driving trends, for example.

“Right now, in this country, for every case we report, we get 1.5 cases back into the laboratory.”

Matthew Gamette

Recommendations:

- Allocate more of the President's budget to fund forensic science, authorize and appropriate the Coverdell and Capacity Enhancement and Backlog Reduction Program (CEBR) grants at higher levels, and increase funding for law enforcement grants, such as the Edward Byrne Memorial Justice Assistance Grant to fund forensic labs;
- Fund foundational or applied research or technology transfer, instrumentation and personnel for forensic disciplines, and national training centers and programs on the federal level;
- Provide comprehensive forensic evidence collection and package training programs for law enforcement taught by forensic science practitioners at POSTs or through partnerships with the Office of Justice Programs (OJP) funded Regional Information Sharing Systems (RISS) network;
- Facilitate the means for officers to ask questions of lab scientists in real-time to ensure the quality application of field instrumentation for drug detection, DNA, and breath alcohol testing;

- Fund more scientists, bigger facilities, and the use of technology like the National Institute of Justice (NIJ) West Virginia University (WVU) FORESIGHT tool, which combats DNA backlog by calculating the lab staff needed to get a desired turnaround time;
- Evaluate submission policies collaboratively (triage teams, labs, investigators, and prosecutors) to determine what is needed for investigation and prosecution in order to control backlogs;
- Employ all forensic disciplines, such as standard toxicology testing for drug-facilitated sexual assault, rather than just DNA analysis;
- Develop an electronic data exchange between law enforcement, labs, and court case management systems, so labs know when investigations have stopped or ended.
- Require and fund state accreditation of forensic providers and certification of forensic scientists;
- Exploit forensic data for criminal intelligence by creating focus groups to develop infrastructure that shares data from labs with fusion centers, High Intensity Drug Trafficking Area's (HIDTA), and state and federal agencies;
- Consider the recommendations of the recent OJP report on Promising Practices in Forensic Lab Intelligence to mine forensics for criminal intelligence;
- Create working groups for sexual assault in each state with more trained sexual assault nurse examiners (SANE) and sexual assault response teams (SART), and funding for state-level SANE and SART coordinators;
- Ensure evidence collection for sexual assault are done by trained nurses;
- Develop sexual assault kit tracking systems in each state;
- Perform an independent audit of how many kits each has, where those kits are located, and the lab status of every kit;
- Develop a mechanism to notify survivors of their kit location and testing status;
- Create national standardization of rape kits to eliminate state-to-state variations;
- Develop lab infrastructure to process all kits, test all probative evidence per kit, and enter all eligible samples into the Combined DNA Index System (CODIS), which is done in public laboratories; and
- Document law enforcement actions to follow up and resolve CODIS hits.

“As identified in the NIJ 2019 Forensic Lab Needs Assessment Report to Congress, forensic labs require a minimum of an additional \$640 million annually to balance incoming requests with reports.”

Matthew Gamette

Second Panelist: Kim Garrett, CEO and Founder of Palomar, Oklahoma City's Family Justice Center

Highlights:

- The family justice center model began in San Diego in 2002 and rapidly grew into a best practice and evidence-based model. There are more than 130 family justice centers across the United States.
- In 2015, Oklahoma City Police Department brought agencies together, under one roof, to form the first integrative collaborative in the community to help victims of domestic violence, sexual assault, and stalking. Previously, professionals working the same case did not work together or even meet and families were unintentionally falling through the cracks, which created more cases.
- The collaborative model brought diverse professionals together, such as: prosecutors, child and animal welfare, mental health, local police departments, sheriff's offices, the U.S. Attorney's office, U.S. Marshalls, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and dozens of non-profits including advocates, civil/legal groups, food and basic needs organizations, child care, therapy, and medical and forensic services working collaboratively in one building.

- Partners have said that what used to take seven weeks of coordinating between professionals now takes seven minutes, thanks to physically working in the same location.
- High-risk team meetings are conducted regularly to ensure a rapid collective response on cases with high lethality.
- Law enforcement leadership was directly related to a high level of success and the city recently approved a \$38 million expansion for this model.
- Partnering in 2018 with the U.S. Attorneys' office, Western District, allowed for these initiatives:
 - Enforcing implementation of Title 18, Section 922 which federally prohibits domestic violence abusers who are subject to a victim protective order or have been previously convicted of a misdemeanor of domestic violence, from possessing a firearm. This is significant as the presence of a gun in a domestic violent situation increases the risk of a homicide by 500 percent.
 - Revitalization of Project Safe Neighborhoods (PSN), a grant that was used to reduce violent crime. It was used to develop "Operation 922" that brought together Assistant United States Attorney (AUSA), ATF, U.S. Marshalls, local law enforcement, state prosecutors, and non-profit advocates.
 - PSN funds paid for the state prosecutor who is cross-deputized as an AUSA. Other funds were used to cross designate a law enforcement officer with ATF.
 - Outcomes to date include 99 cases charged, with 85 found guilty and an average sentence of 81 months. Thirty-five percent of those offenders were known gang members and more than 153 firearms were seized.
 - There are dozens of successes and lives have been saved because of this partnership because federal entities can move for detention immediately until trial, so defendants are not able to bail-out and harass, intimidate or injure their victims. Since the prosecution is based on possession of a weapon, victims do not have to cooperate or testify, which reduces their trauma while simultaneously increasing their safety.
- Federal funding requires many agencies to collaborate, but there are direct policies preventing or greatly restricting information sharing. An example was a recent triple homicide in Oklahoma that was domestic-related. ATF reached out to advocates to see if the victim disclosed anything that could be helpful in the investigation. Advocates could not have predicted this request and, since they did not specifically have a release for ATF, they could not share information.

“If one person in the family chooses to use violence, within four generations, 18 people will continue the cycle.”

Kim Garrett

Recommendations:

- Make the family justice center model a priority for long-term federal funding, ideally including the use of multi-agency teams, which include a prosecutor, therapist, civil/legal attorney, detective, and advocate;
- Develop and fund a federal task force of diverse leaders from professions who interface with crime victims, including law enforcement, attorneys, medical professionals, advocates, and therapists;
- Work together to develop a shared informed consent and information sharing policies and rules for collaborative models; and
- Increase federal resources to support state and local efforts in combatting domestic violence through PSN.

Third Panelist: Richard Hertel, Prosecuting Attorney, 80th Judicial Circuit, Ripley County, Indiana

Highlights:

- Ripley County is a rural and small jurisdiction with a population of about 30,000. The prosecution office has only four attorneys that screen cases, meet with victims, and handle arraignments, plea hearings, and sentencings.
- Domestic violence cases have heightened the degree of witness intimidation and involves power and control dynamics that are not found in crimes more generally, including the fact that the victim still shows loyalty to his or her perpetrator which often leads to recantation of the crime.
- Sexual assault is different from other crimes in that the victim is dealing with an acquaintance, a friend, or an intimate partner using weapons such as drugs or alcohol instead of knives or guns.
- Sexual assault cases require an understanding of trauma and the neurobiology of trauma and that trauma effects everyone differently.

Recommendations:

- Train law enforcement officers the dynamics of domestic violence, and how to be meticulous in evidence collection and, gathering witness statements; the trauma and the neurobiology of trauma and that trauma effects everyone differently; and how to dispel myths about sexual violence;
- Train officers and law professionals on methods of keeping victims engaged in their cases;
- Train prosecutors on when and how to file pre-trial motions that protect victims, including knowing what is admissible and what is inadmissible;
- Train prosecutors on how and when to file protective order violations, bond revocations, rape shield protections, and motions to allow admissible hearsay into trial;
- Train prosecutors on when and how to admit evidence of 404(b) which is a prior bad act of the defendant. This exposes the defendant at particular times and when appropriate;
- Train officers and law professionals on investigating and prosecuting alcohol-facilitated sexual assault, as alcohol is the most common weapon used in sexual assault, there is a lack corroborating evidence, and juries often don't believe victims when alcohol is involved;
- Develop specialized prosecutors or law enforcement to respond to domestic violence or sexual violence instead of general crime. A small office may have a person that handles all sexual violence and human trafficking as well as the child abuse cases.
- Engage in meaningful multi-disciplinary collaborations involving law enforcement, prosecutors, advocates, and medical examiners to share resources and data to educate each other for needed evaluation and adaption. The idea is to find out why these cases are not being reported, why prosecutors aren't filing them, why these cases are being dropped, or why they're being lost from a state's standpoint;
- Require every county or jurisdiction to have a SART that the prosecutor would oversee;
- Recognize, prevent, and respond early to witness intimidation. Law enforcement needs to let victims know what witness intimidation is and how they can go about reporting it in a safe and secure manner. Prosecutors need to be filing additional charges for violations;
- Ensure unbiased and well-informed standards for charging and prosecuting sex crimes cases;

“Partners have said that what used to take seven weeks of coordinating between professionals now takes seven minutes, thanks to physically working in the same location.”

Kim Garrett

- Develop a comprehensive and measurable definition of success in a sexual violence case; and
- Prevent victim-blaming from defense attorneys that is focused on the offender rather than the victim.

Fourth Panelist: Chief Robert Hawkins, Chief of Policy, Muscogee Creek Nation Light Horse Tribal Police Department, Oklahoma

Highlights:

- The Muscogee Creek Nation tribal boundaries span 11 counties, approximately 7200 square miles. The total population in the metropolitan area of Tulsa is about 1.1 million.
- Figuring out jurisdictional bounds is rather complex when it comes to investigating domestic violence and sexual assault cases on tribal land. The following factors are considered:
 - Tribal law enforcement jurisdiction consists of restricted and trust lands and properties held by the tribe.
 - The location of the crime determines which law enforcement agency, whether it's tribal, state, or federal, has jurisdiction.
 - Jurisdiction is also determined by who is involved in a crime; by whether the crime is committed by a native on a non-native, a native on a native, a non-native on a native, or a non-native on a non-native.
 - The tribal agency responds to all calls outside of jurisdiction when it comes to its citizens.
 - Cross-deputization with most of the municipal and county law enforcement agencies within the Creek Nation boundaries helps with issues of jurisdiction.
 - The Violence Against Women Act allows a tribal agency to prosecute a non-native perpetrator who committed a domestic violence and/or sexual assault on a native female victim. Last year the Muscogee Creek Nation was the first tribe to successfully prosecute a non-native suspect in tribal court on domestic assault against a female tribal citizen.
- While on scene tribal officers and the advocates take these steps:
 - Perform a lethality assessment on the victim and take them for a medical check if needed.
 - Make sure the victim is safe at their home or take them to a shelter.
 - If a sexual assault has occurred, then the victim is advised of procedure, and if consent is given, the victim is taken to the tribal medical center, where a sexual assault exam is conducted by the tribe's certified SANE nurse.
- The tribal investigations division is immediately called to the scene to process as follows:
 - Evidence is collected and properly stored as long as possible during the investigation. This includes a chain of custody and a thorough documentation of all evidence.
 - All evidence, including the rape kit, is collected and stored in the evidence room until it can be sent to the lab for analysis. The standard practice is that it is sent within 24 hours.

“To this date, we have a 92% solve rate on sexual assault and a 90% solve rate on domestic violence.”

Chief Robert Hawkins

- Any evidence or information gathered at a scene, whether a domestic violence or sexual assault case, and whether jurisdiction lies with the local or state agency, a report is generated, and all items and documentation is turned over to that agency.
- For sexual assault cases, which fall under the Federal Major Crimes Act, tribal investigators contact the FBI and relay all evidential information to them, as required by federal law.

Recommendations:

- Provide advanced training for law enforcement officers on handling domestic violence and sexual assault cases;
- Ensure victims receive protection from harm from law enforcement and the law by helping victims with protective orders and/or a safe haven;
- Issue watch orders on residences of the victims to increase victim and increase community patrols;
- Encourage victims to report crimes when they happen, so perpetrators are apprehended and prosecuted to the fullest extent of the law;
- Encourage victims and witnesses to cooperate with officers and investigators so that a solid case can be made against the perpetrator;
- Hold all offenders accountable for their actions; and
- Strengthen trust between law enforcement and the communities they serve through regular engagement and use that trust to communicate how law enforcement can help victims of domestic violence or sexual assault.

April 14 Question-and-Answer Period

- Q.** What are your thoughts on the Lethality Assessment Protocol (LAP), and should it be used nation-wide?
- A.** It is a very useful tool for investigations that gives a better idea of what happened and is helpful when filling out the report used by prosecution. It should be implemented across the nation. If it was a requirement that law enforcement do LAP on scene that would be beneficial. In Oklahoma, state law requires a LAP be conducted, and if survivors screen to a certain level of risk, they are connected on scene immediately with advocates. Some information from the LAP helps detectives; such as if any were children involved, which means additional charges may be added. LAPS increase victim safety by connecting them with resources on site. The only backlash is some officers don't like people using their personal cellphones on scene. Police departments could issue department cellphones.
- Q.** What is the general consensus of the forensic community regarding increasing crime lab capacity on rapid DNA?
- A.** The forensic community works very hard to get legislation passed federally to implement the rapid DNA technology into crime laboratories and into booking stations and other venues. The technology is still developing and evolving. There is also support for the FBI's initiatives to make sure that that technology is implemented well into, not only the forensic science community, but also into law enforcement applications to make sure the technology is not misidentifying someone.
- Q.** During the current COVID-19 stay-at-home orders, there has been an increase in domestic violence calls. Do you have any recommendations on what we can learn in real-time to better protect the victims of domestic violence, especially during this pandemic and in the future?
- A.** Some survivor advocacy services have pivoted and started providing texting services and drive-up opportunities for clients to get basic needs and forms. These services have also had to work hard to get the word out, including through law enforcement partnerships, that that they are still open and providing services.
- Q.** How can we improve relationships between federal and state labs? How could there be better communication of case statuses with labs to cut down on unnecessary testing or unnecessary labor and help with the crime lab backlog?
- A.** It is really important that laboratory information management systems work with the law enforcement and the court systems. Labs need to know when court cases resolve so they do not test unnecessary cases. Laboratory information management systems, can help prosecutors, courts, and law enforcement agencies can see what's going on with cases. For instance, once an evidence is received in the lab, it's logged electronically, and then others can see the case status, the analyst that's working on it. Law enforcement, prosecutors and the courts have immediate access to all of that data, so that they knew how long to anticipate that their case would be in the laboratory and when they could expect results.

Technology Issues Encountered by Law Enforcement Panel, April 15, 2020

First Panelist: Darrin Jones, Executive Assistant Director for Science and Technology, FBI

Highlights:

- There has been a steady erosion of law enforcement's ability to access electronic evidence and conduct 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, including complex user controlled encryption, offensively that ensures that no one other than the users can readily or timely access the contents of communications or other stored data.
- 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.
- Technology is being used to dictate the national core value rather than ensuring the national core values that drive and implement technology.
- In a recent gang task force case, source reporting and traditional telephonic intercepts indicated that the main subject suspected of ordering the homicide of another drug dealer used FaceTime to discuss and coordinate criminal activity with his co-conspirators, because this product, designed and implemented by Apple, employs end-to-end encryption.
- In a recent ODETF 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.
- In 2019, Facebook Messenger, sent over 15 million tips to the National Center for Missing and Exploited Children, which immediately forwarded those tips to state and local law enforcement agencies across the U.S. These tips helped to rescue thousands of exploited children.
- Mr. Zuckerberg announced that he intends to encrypt Facebook Messenger soon. What that means is that he 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.
- 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.

“In 2018, Facebook submitted nearly 12 million cyber tips related to child exploitation and child sex trafficking, specifically associated with Facebook Messenger.”

Darrin Jones

Recommendations:

- Enact federal legislation to compel major technology companies to design for themselves strong encryption regimes for their products and services that protect privacy but that also permit lawful access for law enforcement that is pursuant to the due process of law.
- 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.

Second Panelist: Cyrus R. Vance, Jr., District Attorney, New York, NY

Highlights:

- The single most important challenge in the decade is the expanded use of mobile devices by criminals to plan, execute, and communicate about crimes.
- 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. 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, Apple and Google effectively upended centuries of American jurisprudence, holding that nobody's property is beyond the reach of a court-ordered search warrant.
- The Office of the District Attorney Cyber Lab receives on average 1600 mobile devices each year with almost half of those being Apple devices;
- The percentage of locked Apple devices has increased substantially over five years, from 60% in 2014 to 82% in 2019.
- More than 50% of the mobile devices that were received by the District Attorney's office were connected to investigations into crimes of violence such as homicide, sex crimes, and assaults.
- The Office investigated 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.
- The inmate is quoted on the prison recording devices as saying to his associate on the outside, "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."

“There was a babysitter at a local church in Manhattan, who was identified as having shared images and child sexual assault online.....the babysitter was convicted of predatory sexual assault.”

Cyrus R. Vance

Recommendations:

- Federal legislation is necessary to break the encryption stalemate that prevents law enforcement from obtaining evidence subject to a court-ordered search warrant from a smartphone and social media giants; and
- Urge tech companies and law enforcement to meet on a regular basis to discuss lawful access and define paths forward.

Third Panelist: Chuck Cohen: Vice President, The National White Collar Crime Center

Highlights:

- Offenders gravitate to and will seek out platforms where their intended victims spend time.
- Dark web technologies are being used with increasing frequency during the normal course of business, state, local, territorial, and tribal law enforcement and inadvertently encounters the sexual exploitation and trafficking of children.
- Unbeknownst to some financial institutions, they are used by offenders to conceal proceeds of unlawful activity and launder money.
- 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.

“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 a forensically sound manner when investigating these types of child victimization”

Chuck Cohen

Recommendations:

- Update the Communications for Assistance to Law Enforcement Act (CALEA) to require internet service providers to provide assistance to law enforcement similar to that which CALEA currently requires for landline and cellular carriers;
- Increase on a large scale funding and availability of consistent and high quality training and technical assistance for state, local, territorial, and tribal law enforcement that is related to issues outlined in this testimony;
- Implement regulations and laws that require internet service providers and companies providing commercial virtual private networking services to retain certain records, including articulating record retention periods; and
- 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.

Fourth Panelist: Bryan Stirling, Director, South Carolina Department of Corrections

Highlights:

- There was a case in South Carolina where a correctional officer, Captain Robert Johnson, who worked at the Lee Correctional facility, was targeted and shot in his home at point blank range because he was doing his job to find contraband cell phones. The hit was ordered from prison via a contraband illegal cellphone.

- The federal government can jam calls but the states cannot.
- It was not contemplated that states could not block cell phones, thereby protecting citizens from people that have been sentenced and are committed to prison.
- Bryan Stirling was given special authority as a special US Marshal to conduct, along with the Department of Justice and others, a jamming test at one housing unit of a South Carolina prison. This jamming test took place in a dorm with inmates. During the test, it was demonstrated that microjamming of just that one specific location could be accomplished with no bleed over outside of that dorm.

“The hit was ordered from prison via a contraband illegal cell phone.”

Bryan Stirling

Recommendations:

- Get the industry on the record to discuss their technology in order to remove cell phones from prisons;
- Change the federal communication interpretation of the Communications Act of 1934 that currently prohibits states from blocking calls;
- Support statutory changes that would allow states to jam just like the federal prisons are allowed to jam;
- Create a pilot project to allow and evaluate jamming in four states; and
- Explore how state prisons use IMSI-catchers to identify the phones that are illegally used inside prisons.

Fifth Panelist: Todd Craig, Chief, Office of Security Technology, Federal Bureau of Prisons

Highlights:

- Contraband devices get into prison a number of ways, such as inside people and objects, and thrown over fences.
- Increasingly, drones are used to drop contraband devices into prisons and compromise staff.
- A number of other securities technologies are employed to interdict cell phones, such as whole-body imaging devices, sophisticated walk-through metal detectors, thermal fencing, K9 units, and fixed sensor and handheld radio frequency detection.
- There are always issues with staff safety when they are physically locating and removing contraband devices.
- Last year, more than 8,000 contraband devices were recovered and brought to prosecutors and the US Attorney's Office: there are now more than 700 cases for potential prosecution.
- This year, there are more than 1,000 phones recovered from both secure and non-secure facilities.
- 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.

“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.”

Todd Craig

- Managed access is a distributed system of radio frequency antennas that capture all cellular signals, and allows only known signals to go through. A managed access system can capture all cellular signals within the geospatial confines of prison and then disable 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 and does not interfere with signals outside the perimeter. It does not provide intelligence for internal prison security.
- The Bureau of Prisons 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.
- Successful micro-jamming tests were conducted in January 2018, in collaboration with the National Telecommunications Information Administration (NTIA), the Department of Justice Office of Legal Policy and others, at an institution in Cumberland, Maryland.
- At the Federal Corrections Institution in Fort Dix, New Jersey, 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.

Recommendations:

- Ask NTIA and the Federal Communications Commission to support spectrum use requests from correctional agencies to deploy micro-jamming, managed access, and mobile managed access interdiction technologies.
- Facilitate federal state, and local funding for contraband cellular interdiction technologies, including micro-jamming, as a matter of public safety and make statutory changes necessary to effectuate deployment of these technologies.
- Encourage the wireless industry to cooperate with corrections and law enforcement in developing low-cost, innovative wireless interdiction technologies to remove the threat of contraband cell phones from more than 7,000 federal, state, and local jails and prisons across the United States.

April 15 Question-and-Answer Period

Q: You had mentioned in your statement that you'd met with some elected officials regarding lawful access. Give the commission some insight on the barriers that those you met with might have moving forward on lawful access legislation?

A: 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 before Senate committees. The bloom is off the rose, so to speak, with regard to tech companies. Several years ago, tech companies claimed privacy was what they were selling with their products, and now we know that while touting privacy, they were also mining their customers' private information and marketing it to third parties for billions of dollars a year. I think there is now a greater appetite to take stronger and more concrete measures to achieve a federal solution.

Leveraging Technology to Reduce Crime Panel, April 16, 2020

Mr. Phil Keith, Chair, discussed that the focus is on Leveraging Technology to Reduce Crime. The four panelists were Tom Ruocco, Chief of Criminal Investigations Division, Texas Department of Public Safety; Chief Bill Partridge, Oxford, AL Police Department; Christopher Amon, Chief of Firearms Operations Division, Bureau of Alcohol, Tobacco, Firearms and Explosives; and David LeValley, Assistant Chief, Detroit Police Department.

First Panelist: Chief Tom Ruocco, Texas Department of Public Safety

Highlights:

- The Texas Department of Public Safety conducts statewide investigations against criminal organizations involved in drug trafficking, human trafficking, illegal gang activity, fraud, cargo theft, human smuggling, vehicle theft, and illegal gambling. It utilizes sophisticated technology and software-driven analytics to identify criminals and combat criminal activity.
- When deploying new technologies and datasets, law enforcement agencies should use frameworks to assist with decision making that are general enough to be applied across a broad range of technologies, yet specific enough to ensure that agencies consider at a minimum, the predictable costs and risks with the technology. At a minimum, they should consider capability and functionality implications, legislative and regulatory implications, public and law enforcement implications, financial and privacy implications and governance and cybersecurity implications.
- The framework could also be informative when considering the new potential use of technology. For example:
 - During the current COVID-19 pandemic, some European government agencies are utilizing aircraft systems to conduct quarantine checks and monitor social distancing policies.
 - In the United States, a local, state, or federal agency considering similar use for a drone's framework before deployment would be made aware that residents in a specific city raised concerns for their privacy. Drones that were equipped with loudspeakers were used to broadcast a prerecorded warning message to individuals observed violating the COVID-19 social distance policies.
 - In the Golden State killer case where law enforcement effectively leveraged forensic genealogy data initially collected by a private entity to trace people's ancestry to identify a suspect in a cold case.
- New and sophisticated data aggregation and analysis techniques such as artificial intelligence may imbue unique attributes and values to data not anticipated when it was first collected or obtained.
- Well-established cybersecurity frameworks and data handling best practices must be utilized to safeguard the security of the original datasets.
- The frameworks recommended do not dictate or prescribe how 18,000 law enforcement executives will use it.

“If we are continue to succeed in this rapidly evolving digital technology, we must consistently consider new technology and use of datasets.”

Chief Tom Ruocco

Recommendations:

- Employ a consistent and comprehensive framework when considering the adoption and implementation of new technologies. The technological ecosystem is rapidly evolving. And the expansion of communication technology makes collecting evidence much more complicated than ever before; and
- Employ a consistent and comprehensive framework when considering the creation or use of new datasets. Other datasets may be obtained from sources outside an agency such as commercial advertising data and data from vehicle maintenance systems.

Second Panelist: Chief Bill Partridge, Oxford, Alabama

Highlights:

- Five years ago, the department started to try to understand how to best utilize law enforcement technology and personnel to fight and lower crime.
- The department created a regional crime center which now consists of 28 agencies throughout the north-central area of Alabama, serving around 300,000 citizens.
- The crime center itself uses an array of different types of technologies such as license plate readers, pole cameras, trailer cameras, voice-to-text technologies for inmate cellphone calls, and calls through the Sheriff's offices.
- As a result, there have been drastic reductions in crime, such as homicides, home invasions, burglaries, and gun crime.
- The department uses phone and computer forensic labs, video enhancement software, facial recognition, a mobile lab for computer and phone forensics to respond to crime scenes, firefly gunshot detection and ballistic analysis using the National Integrated Ballistic Information Network (NIBIN).
- In Alabama, the average size of the law enforcement agency is ten officers or less. It was essential to bring in smaller departments who cannot afford high-level technology used to counter crime activity.

“And what we have seen over the last year ... of its use is ... dramatic decreases in crime, especially violent crime, across this region.”

Chief Bill Partridge

Recommendations:

- Combine multiple agencies and jurisdictions into single regional entities.
- Fund more small jurisdictions rather than directing most funding into major metropolitan areas.
- Find and fund agencies across the country that would be able to host a regional crime center.

Third Panelist: Chief Christopher Amon, Firearm Operations Division at the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF)

Highlights:

- Crime gun intelligence (CGI) has revolutionized the ability to zero in on the small portion of firearms that

will fall into criminal hands and the violent offenders that perpetrate these crimes. CGI is the collection and analysis of all information related to the unlawful use, possession, or transfer of these firearms.

- The foundation of any crime gun intelligence program is rooted in technology, specifically National Integrated Ballistic Information Network (NIBIN) technology.
 - The NIBIN network is a collection of digital, ballistic images of cartridge cases recovered from crime scenes and crime gun test fires.
 - Technicians review images of the cartridge cases' markings; they correlate them against the database of millions of other images to make associations and link shooting incidents.
- The technology began to improve in the year 2012, with the creation of high definition 3D images, which allowed NIBIN technicians and firearm examiners to create high-confidence correlations.
- Another significant development between 2012 and 2014 remains that more departments started conducting comprehensive collection, which is the gathering of evidence from all shooting scenes regardless of the severity of the crime.
 - This act brought more evidence into the database for comparison. It resulted in more leads with seemingly less critical crimes holding the essential piece of information to solve more serious crimes.
- Academic studies of shooting events linked by NIBIN show a high likelihood of shooters engaging in gun violence multiple times in a short period.
- The ATF created the NIBIN National Correlation and Training Center (NCTC) in Huntsville, which remotely reviews correlations and returns leads to investigators within 48 hours.
 - The NCTC has generated more than 67,000 leads since March of 2016.
- The ATF created minimum standards on the program that mandate NIBIN sites enter cartridge cases within two business days, conduct a correlation review in two business days, and distribute a lead within 24 hours.
 - ATF established 25 crime gun intelligence centers to serve as a clearinghouse for all intelligence related to NIBIN, and other sources.

“Since 2014, acquisitions are up almost 53%, and have gone from 800 leads a year in 2014 to more than 67,000 in 2019.”

Chief Christopher Amon

Recommendations:

- Require all U.S. law enforcement agencies to participate in NIBIN. When one jurisdiction participates, but a neighboring jurisdiction does not, valuable leads disappear;
- Mandate the collection of all fired cartridge cases and test fires from all recovered firearms;
- Facilitate ATF and law enforcement agencies working together to establish dedicated investigative assets targeting violence;
- Utilize ATF's DNA tool to solve violent crime;
- Make grants to state and local laboratories to add more scientists, grow facilities' footprint and fund additional DNA instruments;
- Expand federal laboratories to meet the needs of the federal caseload; and
- Invest in software for investigators to help to aggregate and analyze different crimes and intelligence sources.

Fourth Panelist: Assistant Chief David LeValley, Detroit Police Department (DPD)

Highlights:

- In 2015, Project Greenlight began as a response to counter multiple car-jackings and robberies that were occurring at gas stations and liquor stores.
- DPD partners with businesses that agree to make specific improvements to their sites at their own expense.
 - These include the installation of at least four high definition cameras positioned at entry and exit points, and parking lots.
 - The business owners also agree and provide, at their own expense, increased internet capabilities and 30 days' of cloud storage for the video footage, which is capable of being viewed remotely by the police department.
- The police department agrees to virtually patrol the location from a real-time crime center, provide priority response both virtually and in-person calls of the areas, make unique attention visits to the sites, and advertise the program for increased awareness.
- The program started with eight gas stations and now consists of 600 participating businesses and is still growing every day.
 - Law enforcement now has access to over 2800 live high definition camera feeds.
 - At the eight original locations, there has been a reduction in violent crime at 44.9 percent, when comparing the years 2015 to 2019.
- Gas stations in the program have seen a decrease of 25.3% during that time, while the entire city has seen a 16% reduction during that time.
- In 2015, there were 3,648 robberies and 523 car-jackings that were reduced to 2,377 robberies and 244 car-jackings by 2019.
- Detectives have access to 30 days' of footage, which they are able to use to ensure case closures.
- License plate readers consist of deploying high-speed cameras throughout the city that capture every license plate that passes.
- The Facial Recognition Program is a probe image of a suspect believed to have committed a violent offense such as murder, robbery, rape, or aggravated assault.
 - Facial recognition matches are just investigative leads, and detectives still have to conduct their investigation to establish probable cause before an arrest.

“Law enforcement now has access to over 2800 live high definition camera feeds.”

Assistant Chief David LeValley

Recommendations:

- Invest in technology infrastructure that enables the programs like Project Greenlight to work, particularly through grant funding geared towards getting fiber or wireless access at fast speeds, which can be very costly and prevent municipalities from taking on new technology programs;
- Encourage transparency. It is easier for law enforcement to be open and transparent about the use of technology to its citizens rather than let media or critics expose it;
- Mandate training and certifications for technologists and analysts;

- Mandating universal certifications and training will protect both law enforcement agencies and the public from misuse; and
- Increase technical assistance.
 - Facilitating technical assistance and peer exchanges with other law enforcement agencies would be useful.

April 16 Question-and-Answer Period

Q: How did you initially fund the processes you had to go through and get in the buildings and pulled together for your Regional Crime Center?

A: Five years ago, our mayor and City Council stepped up to the plate and paid for the center.

Q: Other than the Metro Crime Center in Birmingham and East Alabama, do you know of any others that are on the forefront in Alabama or adjoining states?

A: Chief McMurray in Huntsville is in the process of building-out the North Alabama Metro Area Crime Center. Tuscaloosa is also in the process of obtaining funding to start its Crime Center.