Testimony of
Gerard Keegan
CTIA

Before the Oklahoma Senate Interim Study Committee on
Cellular and Electronic Devices in Oklahoma Prisons

October 21, 2019

Chair, Vice Chair, and members of the committee, on behalf of CTIA, the trade association for the wireless communications industry, thank you for the opportunity to testify about the wireless industry's efforts to help the corrections community combat the problem of contraband devices in our nation's correctional facilities.

We fully support policymakers' efforts to keep contraband wireless phones out of correctional institutions. Wireless carriers have no legitimate subscribers imprisoned or detained in correctional facilities and no interest in seeing the unauthorized use of wireless devices in these facilities. We are dedicated to continuing our work to develop and implement measures to help solve this problem while preserving the ability for law-abiding members of the public to continue to reliably access the wireless services provided by CTIA's member companies.

The wireless industry has devoted significant resources and funding to help combat this problem. In 2018, we formed a task force consisting of corrections officials, wireless carrier representatives, and CTIA staff to coordinate an in-depth examination of potential technological, legal, and administrative solutions to contraband device use in correctional facilities. As part of the task force, we brought on Dr. Charles Clancy to administer a test bed of Contraband Interdiction System (CIS) technologies, including jamming. Dr. Clancy was a professor of electrical engineering at Virginia Tech, where he was a Senior Fellow at the Hume Center for National Security and Technology. Prior to

joining Virginia Tech, he led wireless technology research programs at the National Security Agency. In that role, he worked on a range of cell phone-related programs. Dr. Clancy is an internationally recognized expert in wireless security, has chaired standards committees within the IETF and Wireless Innovation Forum, and has testified before Congress.

The task force has held a number of meetings over the past year and a half and has actively worked to identify contraband phone challenges and potential solutions. In addition to the testbed, the task force worked to develop a model state-level court order process to enable wireless carriers to disable cell phone service to devices identified as contraband. Further, the task force acted to use the industry's stolen phones database to deny service to identified contraband devices. In April, the task force issued a report on its activities to-date.

As noted in task force report, Dr. Clancy and the team from Virginia Tech's Applied Research Corporation (VT-ARC) "conducted extensive outreach to CIS [contraband interdiction system] vendors."[1] Twelve CIS vendors attended a workshop coordinated by the task force and presented their technical details and cost and current deployments. Three providers – two managed access system (MAS) providers and one jamming provider – accepted the task force's invitation to submit their systems for evaluation in the testbed.

The Virginia Tech team developed stringent test plans for lab and field conditions. The team tested two MAS technologies in the field – one at Lee Correctional Institution in Bishopville, South Carolina and the other at the Mark W. Stiles Unit in Beaumont, Texas. The test reports noted that "[t]he two MAS solutions in the Testbed succeeded in interdicting communications from contraband devices

[1] *See* "Contraband Phone Task Force Status Report," *available at:* https://api.ctia.org/wp-content/uploads/2019/04/Contraband-Phone-Task-Force-Status-Report-Combined.pdf (last accessed Oct 16, 2019).

over simulated and actual cellular networks."[2] The report goes on to state that "VT-ARC observed that both MAS solutions were successful in blocking unauthorized communications in most areas of the correctional institution."[3] It did find that one MAS solution did not fully block communication attempts from certain areas of the facility, which were under construction. Furthermore, the testing showed that the MAS providers were "generally contained in the correctional facilities, suggesting that the systems posed little risk to interference to legitimate wireless users beyond the facilities' perimeters."[4]

In addition, VT-ARC performed lab tests of jamming equipment. Because of the legal requirement of federal government involvement, the task force was unable to timely conduct field testing of jammers. VT-ARC's lab testing of jammers, however, found that the jamming equipment tested "indicated that a real-world deployment of this system could cause harmful interference" with commercial wireless service outside correctional facilities, "which may affect 9-1-1 calls and public safety communications on that spectrum."[5] The report did note that additional testing "could more fully assess the likelihood of harmful interference."[6] Moreover, VT-ARC found "the overall cost of this solution may approach that of a MAS solution."[7]

Moreover, the task force report included not only technology assessments and key metrics for each technology tested but also best practices on deployment of CIS technologies. The task force also evaluated legal and administrative practices, including court orders, for directing carriers to take action against contraband devices. CTIA and our members have worked closely to develop a model court

[2] *Id* at 6.
[3] *Id.*
[4] *Id* at 7.
[5] *Id* at 8.
[6] *Id.*
[7] *Id.*

order process that would direct wireless carriers to disable commercial service to a device identified as contraband. The wireless industry has also worked diligently to deploy the stolen phones database for use in combatting contraband devices in correctional facilities. Carriers are able to render SIM cards inoperable, but we have heard that inmates often swap out SIM cards. We now believe we will be able to render wireless service inoperable to a contraband device so that wireless service will not work even if inmates swap out SIM cards. To do this, we extended the existing stolen phone database to contraband devices.

Additionally, wireless carriers are actively working with MAS providers to enter into roaming agreements with those providers. This was a recommendation included in the task force's report. This concept could potentially make MAS deployments less costly for a new installation.

As I hope our recent efforts make clear, helping to eliminate contraband phones in prisons is a wireless industry priority. Over the past decade, CTIA and its member companies have actively worked with managed access and cell detection technology vendors to identify approaches that would curb the use of contraband cell phones in prisons. To facilitate the deployment of managed access systems, wireless carriers have entered into numerous spectrum lease agreements with multiple providers. In addition, we have provided significant technical assistance to these vendors to address operability challenges and prevent interference with cellular networks. We are firmly committed to doing more.

The wireless industry has worked, and will continue to work, collaboratively with various stakeholders, including corrections officials, to address the serious problem of contraband wireless devices. The wireless industry and corrections facilities have embraced managed access technologies as an effective means of preventing unauthorized wireless communications within prisons. While

jamming has been cited as a means of curbing contraband device use, we have concerns with the harmful side effects to the use of jamming technologies. We do support further testing of jamming equipment in the laboratory and the field with participation and meaningful input from wireless carriers.

Managed Access. Managed access and other detection systems have proven effective in combating the use of contraband wireless devices in prisons. Managed access systems are micro-cellular, private networks that analyze transmission to and from wireless devices to determine whether the device is authorized to access public carrier networks. Managed access system base stations capture voice, text, and data communications within the system's coverage area and cross-check the identifying information of the device against a list of authorized devices. If the device is not authorized, communications are terminated. Meanwhile, users of authorized devices may continue to access public carrier networks as they normally would.

To operate managed access systems, operators of these private networks require a right to transmit over valuable commercial mobile spectrum licensed to commercial wireless carriers. Wireless carriers whose licensed service areas overlap the footprint of state or local corrections facilities work with managed access system providers to arrange for access to spectrum. Once consent is obtained from the carrier, a lease application is filed with the FCC to enable managed access system deployment on the carrier's spectrum.

Managed access systems have been deployed throughout the country and are currently used at a number of state and local corrections facilities. The wireless industry favors managed access systems because they block unauthorized communications, reduce incentives for parties to smuggle

contraband phones into prisons, and permit lawful communications to take place without interruption or degradation.

Jammers. Under current law, jamming by non-federal entities constitutes an unlawful interference with radio communications in violation of Section 333 of the Communications Act. Consistent with this law, the FCC has taken swift and forceful action against the users and manufacturers of these unlawful devices. And there are sound policy and technical reasons for this, as jamming has proven it can be an overly blunt instrument and a potential public safety threat. By blocking *all* wireless communications inside and near corrections facilities, legitimate communications – including calls to 9-1-1 - are blocked and, if the jammer fails, corrections officials have no further recourse against users of contraband phones.

Some of our member companies with operations along the border have experienced harmful interference from jammers operating in Mexico and several miles from the border. These jammers are causing destructive interference to commercial and public safety operations across entire U.S. cities on the US-Mexico border. This creates an extremely dangerous situation for lawful wireless users outside prison walls, who may find a critical call to 9-1-1 blocked by a malfunctioning or over-inclusive jammer. Moreover, jamming can disrupt service in the spectrum outside of the targeted commercial band. Public safety radio communications, for example, operating in the 700 MHz and 800 MHz would be put at risk of interference from jammers, given their close proximity to commercial operations in those bands. Because of these issues, we have concerns with the use of cell phone jammers in correctional facilities.

In closing, we stand committed to continue our work with federal and state officials, public safety representatives, and technology providers to combat this problem. Thank you for the opportunity to testify today.