

Attachment A

Contraband Interdiction System Testbed Report & Best Practice Recommendations

Prepared by:



EXECUTIVE SUMMARY

This report describes the Virginia Tech Applied Research Corporation (VT-ARC)'s activities to test and evaluate Contraband Interdiction Systems (CIS) in both laboratory and field conditions. The events occurred between April 2018 and January 2019 in collaboration with CTIA and members of the Contraband Phone Task Force, including CTIA member companies, members of the Association of State Correctional Administrators (ASCA), and the Department of Justice's Bureau of Prisons (BOP).

BACKGROUND

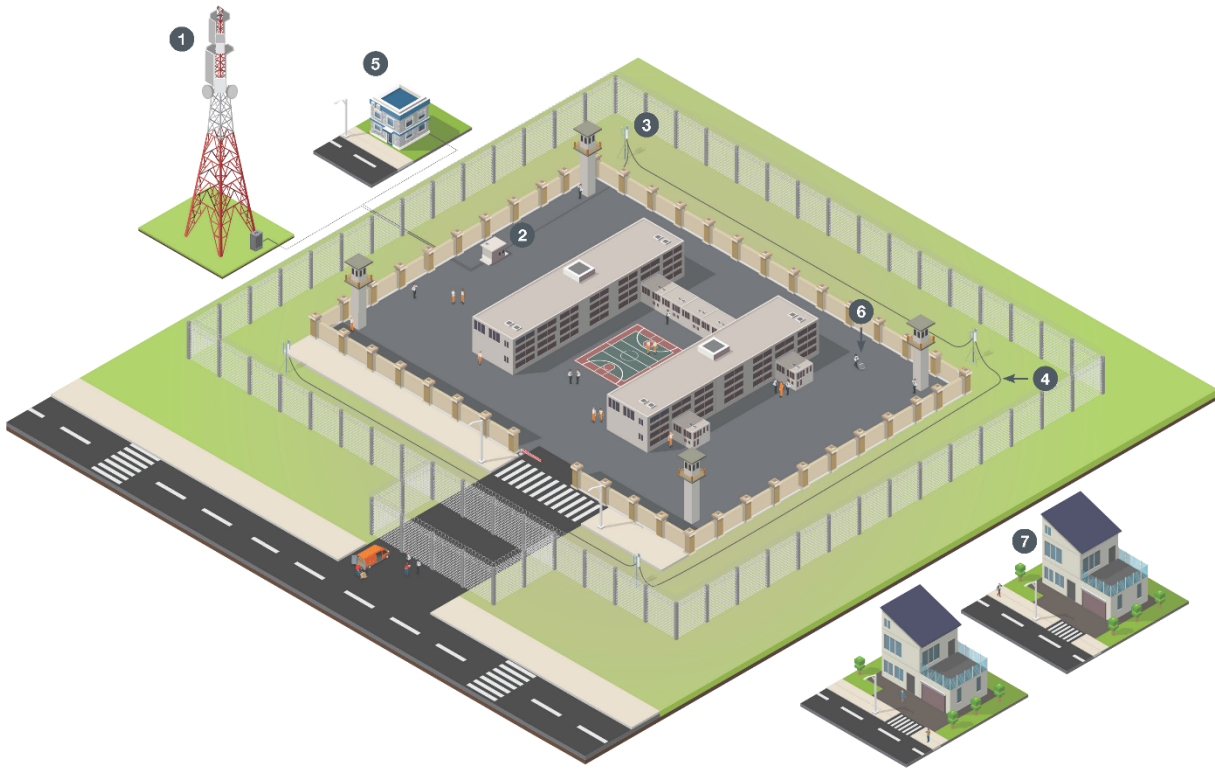
In February 2018, the Federal Communications Commission (FCC), under the leadership of Chairman Ajit Pai, convened a stakeholder meeting to discuss solutions to contraband cell phones in state correctional facilities. Chairman Pai explained the initiative's goal as follows: "to bring together a diverse group to determine the most effective, affordable, and safe ways to address this problem—that is, to stop the threat of contraband cellphones without causing harm to legitimate wireless users." In April 2018, CTIA and ASCA launched the Contraband Phone Task Force.

Through the Task Force, CTIA and the wireless industry set out to work with the corrections community to establish a test bed to assess Contraband Interdiction System (CIS) technologies. CIS technologies are deployed in correctional facilities to combat use of unauthorized mobile phones, and their effectiveness in denying and/or detecting phones is a function of many parameters, including the radiofrequency (RF) environment, type and configuration of phones, and the characteristics of the commercial mobile networks operating in the area. CTIA and the wireless industry demonstrated their commitment to the Contraband Phone Task Force by funding the development and execution of the CIS Test Bed. CIS vendors contributed through their participation in the CIS Workshop and providing equipment, coordination, and collaboration for testing. Additionally, the CIS vendors paid a fee to participate in the testbed.

CTIA and the wireless industry selected Dr. T. Charles Clancy, Bradley Professor of Cybersecurity, Electrical and Computer Engineering from Virginia Tech, and VT-ARC to administer a testbed program that includes both laboratory testing and in-facility testing for CIS technologies. This report summarizes the activities to test and evaluate CIS technologies and provides "best practice" recommendations on their use.

CONTRABAND INTERDICTION SYSTEMS

An overview of elements that can be included in a CIS deployment is provided in the figure below.



Overview of a Contraband Interdiction System

Contraband Interdiction Systems (CIS) detect unauthorized user equipment (UE) and prevent unauthorized communications from escaping a correctional facility. Examples of CIS are Denial of Service Systems (DSS), Managed Access Systems (MAS), and Cell Detection Systems (CDS). CIS deployments are unique, complex installations with multiple components. Common elements of CIS are described below:

- | | |
|--|---|
| <p>1 Cell Tower</p> <ul style="list-style-type: none"> • Provides service to the macro network <p>2 CIS Control Hub</p> <ul style="list-style-type: none"> • Manages all CIS functions • Routes calls, SMS, and data from authorized UEs to the macro network • Blocks calls, SMS, and data from unauthorized UEs <p>3 CIS Antenna</p> <ul style="list-style-type: none"> • Creates RF perimeter around correctional facility • Captures all incoming RF emanations from Cell Towers surrounding correctional facility • Captures all outgoing RF emanations from UEs within correctional facility • Indoor and outdoor options | <p>4 Rigid Conduit</p> <ul style="list-style-type: none"> • Connects CIS Antennas to CIS Control Hub • Built to Law Enforcement Agency specifications to protect against sabotage <p>5 Public Safety Answering Point</p> <ul style="list-style-type: none"> • CIS routes 911 calls from all UEs to PSAP (configurable based on facility requirements) <p>6 Cell Detection System</p> <ul style="list-style-type: none"> • Conducts mobile, periodic sweeps of facility to detect contraband UEs <p>7 Neighborhood in Close Proximity to Correctional Facility</p> <ul style="list-style-type: none"> • Per 47 CFR § 1.9020(n), CIS vendors must notify general public 10 days prior to system activation |
|--|---|

Overview of a Contraband Interdiction System

SUMMARY OF ACTIVITIES

Dr. Clancy and the team from VT-ARC—Mr. Mike DiFrancisco, Mr. Kristoffer Lemoins, and Mr. Adam Gorski—acted as the CIS Testbed Administrator for this project. The CIS Testbed Administrator performed the following major activities:

- Contraband Interdiction System Workshop – 13-14 June 2018
 - CIS Technology Overview
 - Presentations from 12 CIS Solutions vendors
- Contraband Phone Task Force Meetings/Presentations
 - 30 April 2018, Washington DC – Madison Hotel
 - 14 June 2018, Arlington VA – After CIS Workshop
 - 7 September 2018, Arlington VA – Including CIS Testbed Tour/Demo
 - 10 January 2019, New Orleans LA – Before ASCA Winter Meeting
- Call to Participate in the Contraband Interdiction System Testbed & Request to ASCA to provide Locations for Field Testing
- CIS Laboratory Testing
 - One Jammer
 - Two Managed Access Systems
- CIS Field Testing
 - Lee Correctional Institution, SC – Installed MAS
 - Mark W. Stiles Unit, TX – Installed MAS

The VT-ARC CIS Testbed evaluated a jammer (a subclass of Denial of Service Systems (DSS)) and two Managed Access Systems (MAS). Jammers introduce interference into the uplink and/or downlink spectrum bands to prevent signaling between phones and base stations. MAS is a deployment of active base stations within an operational facility, working in coordination with the wireless carriers covering the area, that combine with a whitelist/blacklist feature set to prevent unauthorized calls from completing. A MAS may be deployed using a Distributed Antenna System (DAS) or through a network of small cells. MAS can interface with the telecommunications infrastructure to allow whitelisted and emergency phone calls to be properly routed.

SUMMARY OF LABORATORY & FIELD TEST RESULTS

Test	DSS/Jammer	MAS
RF Denial Mechanism	— Compresses dynamic range of RF channel of phone until denial of service occurs; RF interference overcomes downlink signal synchronization	— Forces handset to step down to 2G where services are blocked — MAS can handle or block LTE / UMTS services without step down; requires carrier roaming agreement (not available in field tests)

RF Denial Performance - Laboratory	<ul style="list-style-type: none"> — Achieved: Dependent on relative power of desired signal — Significant out of band interference present 	<ul style="list-style-type: none"> — Achieved: Dependent on relative power of desired signal — Substantial feature sets providing information and services to correctional facility officials
RF Denial Performance - Field	<ul style="list-style-type: none"> — N/A - Field test not performed due to 47 U.S.C. § 333 and FCC policy prohibition on non-federal jammer operations 	<ul style="list-style-type: none"> — Effective: MAS installed at two large state correctional facilities demonstrated effective control of contraband phone communications — RF coverage design critical to effectiveness — Key features demonstrated (911, allow lists, etc.)

DISCUSSION OF MAS UTILITY

The CIS Testbed received voluntary participation from two MAS technology vendors. VT-ARC tested these two systems in both the CIS Testbed lab environment and in deployed environments at Lee Correctional Institution (SC) and Mark W. Stiles Unit (TX).

The two MAS solutions succeeded in blocking communications from contraband devices over simulated and actual cellular networks. The effectiveness of the MAS solutions depended on the power of the interdiction system’s signal relative to the surrounding commercial cellular networks as well as their coverage of frequency channels used by contraband devices. In its laboratory testing, VT-ARC incrementally decreased the power of the MAS networks until test devices attached to the simulated cellular network, revealing a “crossover” point at which actual contraband phones would evade interdiction. In its field tests, VT-ARC observed that both MAS solutions were successful in blocking unauthorized communications in areas that the correctional facilities required to be covered. However, in isolated areas that were mostly under construction at both field test facilities, VT-ARC observed that some communications from test devices were able to escape the MAS network. In addition, signals from both MAS solutions were contained within the correctional facilities, suggesting that the systems posed little risk of interference to legitimate wireless users beyond the facilities’ perimeters at the time of testing.

Careful design of the RF distribution network is required to ensure MAS deployments do not disrupt customers on carrier networks. At Lee Correctional Institution, instances of local users in Bishopville, SC having their phones “captured” by the MAS were reported. In this case, the MAS vendor was notified and adjusted the MAS to prevent future occurrences. This example highlights the need for careful RF design and routine monitoring of MAS signal levels relative to carrier network levels both inside and outside the prison. Spectrum interference can be minimized using a Distributed Antenna System (DAS) with many antennas transmitting at relatively low signal levels with directivity away from the outside areas of the prison, along with careful and repeated measurement and monitoring.

MAS deployments require significant up-front investment; it follows that vendors require multi-year service contracts to recoup these up-front costs. To guarantee successful contraband interdiction, as well as minimization of disruption to carrier cellular networks, the system must be serviced and supported throughout its lifecycle.

In addition to denying contraband phone access to cellular networks, MAS systems include feature sets that are capable of providing information and services to correctional facility officials, including documentation of each specific instance where a contraband phone attempted to communicate.

Discussion of Jamming Denial of Service System (DSS) Utility

The CIS Testbed only received voluntary participation from one jammer technology vendor. One other Jammer technology vendor participated in the CIS Workshop, but chose not to participate in lab testing despite the solicitation to participate. While the initial VT-ARC project plan included the potential to field test a jamming DSS solution in a prison setting, 47 U.S.C. § 333 and FCC policy bar non-federal operations of jammers that interfere with radio communications of any licensed or authorized stations. This constraint prevented field testing of jammers.

Laboratory testing of one manufacturer's jammer (used as a CIS in overseas prisons) indicated strong potential for this system to create substantial aggregate interference to be generated in a practical prison scenario with multiple jammer units. In a practical real-world deployment of jammers with the characteristic that were tested, harmful interference to commercial cellular services outside a prison is very likely, and there is also a significant risk of out of band interference to other RF-dependent services.

BEST PRACTICES FOR USE OF CIS IN CORRECTIONAL FACILITIES

The successful deployment of a Contraband Interdiction System (CIS) requires the management of multiple factors. These factors are both human and technical. Human factors drive the technical means to defeat human attempts to defeat the system and enhance coordination between CIS vendors and correctional facility officials. Technical factors drive the system's evolution, roadmap, and deployment strategy. Our best practice recommendations below focus on MAS and reflect the field testing that was performed.

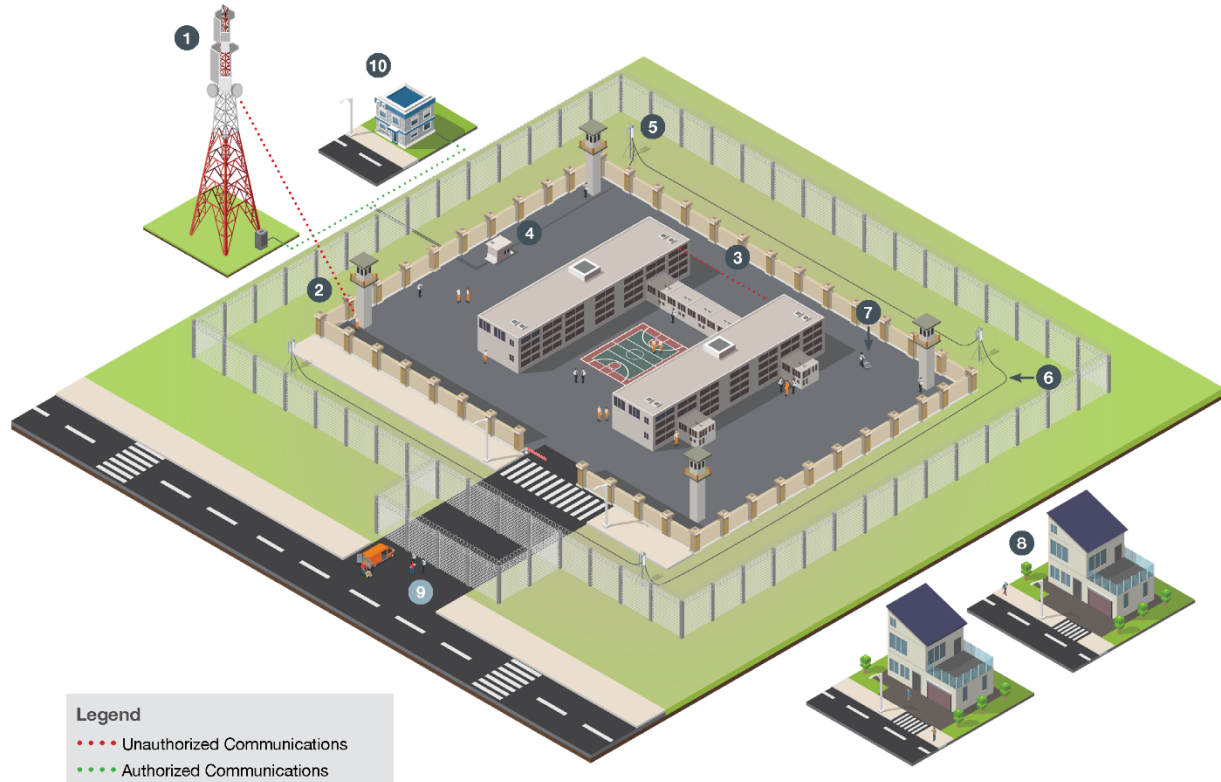
Lab testing of a particular jamming solution suggested that there are significant technical issues associated with deploying a jammer in a correctional facility. Pending substantial additional testing and analysis to prove that another particular system might be deployed in such a way to avoid harmful interference to other systems (both inside and outside a particular prison environment) avoiding jamming would be considered the only best practice for that technology. Some criteria that should be included in such testing and analysis are included in the Recommendations for Next Steps.

The top MAS best practices are summarized below:

- Continual RF planning, testing, and monitoring to ensure control of relative power at correct levels inside and outside the correctional facility.
 - Communication between correctional facility officials, MAS vendors and cellular providers regarding network re-provisioning, inmate activity, and system performance.
- Coordination with general public to address inadvertent RF leakage into the community, prevent spectral interference, and address emergency events (e.g., natural disasters, security incidents)
- Effective control of contraband influx into facilities
- Allow lists to permit authorized communications throughout the facility
- Emergency call and dialed number handling

CIS CHALLENGES

Numerous challenges can occur when deploying a Contraband Interdiction System. While each deployment is unique, a graphic displaying common deployment issues is shown in the figure below.



Challenges for Contraband Interdiction Systems

Contraband Interdiction Systems (CIS) are highly effective at blocking unauthorized communications; however, challenges exist. Below are challenges that are typical to a deployment of a CIS:

- | | |
|---|--|
| <p>1 Cell Tower</p> <ul style="list-style-type: none"> RF emanations can be re-provisioned by cellular providers, rendering CIS ineffective <p>2 Contraband Cellular Communications</p> <ul style="list-style-type: none"> Inmates can find locations within the facility where UEs can connect to a macro network via a Cell Tower <p>3 Contraband WiFi Communications</p> <ul style="list-style-type: none"> Inmates can communicate within correctional facility using contraband WiFi hotspots that the CIS does not capture <p>4 CIS Control Hub</p> <ul style="list-style-type: none"> Contains proprietary information from cellular providers that must be protected Allow list permits communications from authorized UEs to the macro network via the CIS <p>5 CIS Antenna</p> <ul style="list-style-type: none"> Vulnerable to sabotage and weather Can capture corrections officials' UEs and block their authorized communications | <p>6 Rigid Conduit</p> <ul style="list-style-type: none"> Vulnerable to sabotage <p>7 Cell Detection System</p> <ul style="list-style-type: none"> Contraband sweeps can alert inmates to turn off or disable contraband UEs, rendering system less effective over time <p>8 Neighborhood in Close Proximity to Correctional Facility</p> <ul style="list-style-type: none"> RF from CIS can leak into area, causing inadvertent capture of general public communications <p>9 Contraband Influx</p> <ul style="list-style-type: none"> Continued influx of contraband UEs into correctional facility creates escape vectors for inmate communications <p>10 Public Safety Answering Point</p> <ul style="list-style-type: none"> Contraband UEs can call 911 and send non-emergency calls to PSAP |
|---|--|

Common Contraband Interdiction System Challenges

The top critical human and technical issues and recommendations to address them are shown below.

Critical Issue 1: MAS coverage needs to adapt quickly to macro network changes

Communications between MAS vendors and macro network providers vary; when they do not communicate and networks are re-provisioned, the MAS may lose the ability to prevent communications.

Recommendation:

- Ensure MAS vendors monitor and react to cellular macro network changes; consider creating lines of communication between cellular providers, correctional facility officials, and CIS vendors to communicate impactful macro network changes while ensuring practices/guidelines are in place to protect cellular provider proprietary information.

Critical Issue 2: 2G Services ending -- Impact on current MAS designs

A typical means for MAS networks to deny service is to step down the User Equipment (UE), e.g., cell phones and hotspots, from 3G / 4G to 2G services to avoid controlled/encrypted authentication at the higher service levels. Cellular providers are already starting to disable 2G services. At some point in the future, UEs may not include 2G functionality, rendering legacy MAS networks ineffective.

Recommendation:

- Create roaming agreements between cellular providers and MAS vendors to enable newer generation services on MAS networks; upgrade MAS designs to “capture” contraband devices without forcing UEs to 2G.

Critical Issue 3: Correctional officials or individuals on “allow list” cannot always communicate

Corrections officials have issues with communicating with each other in certain areas of the facility, particularly in areas where the MAS network would typically handover to the macro network and in locations within the facility with weaker coverage or in between MAS coverage zones.

Recommendation:

- Pursue a “MAS Evolved” roadmap to transition MAS systems from a single-cell uncoordinated system to one that co-exists with the public macro network to permit authorized hand-offs and communications coordination.

Critical Issue 4: Contraband cell phones are enabling unauthorized inmate communications via WiFi

While the two MAS solutions tested succeeded in blocking communications from contraband devices over simulated and actual cellular networks, a CIS system can only do so much to prevent unauthorized communications from occurring. The MAS that were tested were not required to handle WiFi communications as part of their contracts with the correctional institutions. Contraband WiFi hotspots enable prohibited internal communications within a correctional facility. The contraband hotspots can

also create a bridge between areas with high CIS coverage to those with little or no coverage and provide an escape path for unauthorized communications.

Recommendation:

- Consider enhancing MAS to block WiFi communication and including requirements for WiFi features in MAS procurements. [Note: Blocking WiFi operations on unlicensed spectrum may raise legal issues that require further analysis. On several occasions, the FCC has said that the 47 USC § 333 prohibition extends to Wi-Fi blocking. See, e.g. FCC Enforcement Advisory Warning: Wi-Fi Blocking is Prohibited, Persons or Businesses Causing Intentional Interference to Wi-Fi Hot Spots Are Subject to Enforcement Action, 30 FCC Rcd 387 (2015).]

RECOMMENDATIONS FOR NEXT STEPS

MAS Evolved

The solutions to critical issues 2 and 3 enable a path to a potentially lower cost MAS solution by removing RF coverage complexity within the correctional facility and taking advantage of carrier roaming agreements. The “MAS Evolved” concept would trade RF coverage complexity within the correctional facility for one that takes advantage of carrier roaming agreements.

This MAS Evolved concept would require a partnership between MAS vendors and carriers via roaming interconnect. In addition to potentially being less costly (for a new installation), it has the potential to increase the MAS feature set to provide better service to correctional facilities. Moreover, a lower cost solution based on small cells could potentially provide effective multilateration by the MAS to identify the location of UEs in and near the correctional facility. MAS vendors and wireless carriers could explore a MAS Evolved solution by taking the following steps:

Phase 1: Roaming Interconnect

- Implement a limited standard Diameter proxy for MAS deployments that allows for authentication of handsets
- Define Roaming use-case and best practices

Phase 2: Smallcell Testing

- MAS providers and prison officials should consider testing multilateration precision across a range of scenarios, in collaboration with roaming authentication from carriers
- Conduct field testing in correctional facility environment of small-cell / location services (LCS) approach leveraging roaming interfaces

Future Testing of Different Jamming Solutions – Field and Lab

Laboratory testing of one manufacturer’s jammer indicated a strong risk of generating substantial aggregate interference, both in the designed cellular bands, and out of band. This risk multiplies when

multiple jammer units are used in a correctional facility deployment. Harmful interference to multiple communications domains (e.g., commercial cellular services, terrestrial communications including public safety, satellite communications, aviation, etc.) outside a correctional facility could occur. Although the jamming solution that was tested in the CIS Testbed was not necessarily representative of all possible jammers that may be considered for use in U.S. correctional facilities, this risk has not been thoroughly examined. For example, in January 2018, the National Telecommunications and Information Administration (NTIA) in coordination with the Federal BOP tested a single jammer designed to prevent cellular communication within a single correctional facility cell.¹ NTIA’s report noted that:

“Analysis of the jammer’s potential for harmful interference to licensed radio services, if any, outside the targeted prison cell is beyond the scope of [the NTIA] report.”

Testing additional jamming solutions in both laboratory and field conditions would be needed to more fully assess the likelihood of harmful interference.

If additional tests of jamming solutions were to take place, they should include the following:

- Explicit measurement of aggregate interference from multiple jammers configured to provide useful CIS service to a correctional facility or portion of a correctional facility.
 - What are the interference signal levels inside and outside of the facility?
 - Do the levels outside the facility constitute harmful interference to cell phones operating in public spaces, or to other services operating in adjacent bands?
- Coordination with cellular service providers before, during and after the test to use carrier Key Performance Indicator (KPI) data² to assess the impact of aggregate interference from the jammers at various cell sites in the vicinity.
- Evaluation of the efficacy of jamming as a CIS solution:
 - Do jammers prevent cell phone operations (i.e., connecting to commercial wireless carrier outdoor cells) at appropriate locations inside the facility?
 - What is the range of efficacy: How far from the jammer(s) are cell phones prevented from operating?

Furthermore, to the extent additional field tests occur, it is recommended that the jammers being used in the field tests be provided to a test laboratory independent of the jammer vendor to document the operation and performance in a controlled environment, using measurements such as those detailed in this report.

¹ Reference: NTIA Report TR-18-533, Emission Measurements of a Contraband Wireless Device Jammer at a Federal Correctional facility, June 2018, available at <https://www.its.bldrdoc.gov/publications/download/TR-18-533.pdf>. We note that in early April 2019, BoP conducted an additional jamming test during which NTIA engineers performed measurements of radio emissions to observe and document their characteristics. Reference: U.S. Department of Justice, Bureau of Prisons Tests Micro-Jamming Technology in South Carolina Prison to Prevent Contraband Cell Phones, Press Release (Apr. 12, 2019), <https://www.justice.gov/opa/pr/bureau-prisons-tests-micro-jamming-technology-south-carolina-prison-prevent-contraband-cell>.

² KPI data includes noise measurements (e.g., interference over thermal, receive total wideband power) and performance data (e.g., throughput, connected users).

TABLE OF CONTENTS

Executive Summary.....	i
Background	i
Contraband Interdiction Systems	i
Summary of Activities	iii
Summary of Laboratory & Field Test Results.....	iii
Discussion of MAS Utility	iv
Best Practices for Use of CIS in Correctional Facilities.....	v
CIS Challenges	vi
Recommendations for Next Steps	viii
1 Introduction	1-4
1.1 History & Purpose	1-4
1.1.1 Contraband Interdiction Systems	1-4
1.1.2 Contraband Phones Task Force selection of CIS Testbed Administrator.....	1-5
1.1.3 Summary of CIS Testbed Administrator Statement of Work.....	1-6
1.2 Engagement with Contraband Phone Task Force.....	1-7
1.3 Outreach and Engagement with CIS Vendors.....	1-8
1.3.1 CIS Vendor Workshop	1-8
1.3.2 CIS Workshop Vendors.....	1-10
1.3.3 Vendor Participation in CIS Testbed	1-10
2 Contraband Interdiction System Testing Process	2-11
2.1 CIS Testbed Laboratory Testing	2-11
2.1.1 Context: Taxonomy of Contraband Interdiction Systems.....	2-11
2.1.2 Test Plan – Systematic Lab Testing Approach.....	2-12
2.1.3 Testbed Architecture	2-14
2.2 CIS Testbed Field (Correctional Facility) Testing.....	2-17
2.2.1 Field Testing Approach.....	2-17
2.2.2 Field Test Equipment	2-18
2.2.3 Coordination with Wireless Carriers.....	2-18
2.2.4 Coordination with Correctional Facility & Vendor.....	2-19
2.2.5 Site Survey.....	2-19

2.2.6 Field Test Event2-20

3 CIS Testbed Results Summary.....3-23

3.1 MAS Lab Results Summary.....3-23

3.2 DSS (Jamming) Lab Results Summary3-26

3.3 MAS Field Test Results Summary.....3-30

4 Summary of Findings.....4-53

4.1 MAS Solutions Findings.....4-53

4.1 DSS (Jamming) Solutions Findings4-55

5 Suggested Guidelines and Best Practices.....5-57

5.1 MAS Solutions Guidelines and Best Practices.....5-57

5.1.1 MAS Best Practice Recommendations5-58

5.1.2 MAS Deployment Critical Issues and Related Recommendations.....5-58

5.2 DSS (Jamming) Solutions Guidelines and Best Practices5-60

6 Recommendations for Next Steps6-61

6.1 MAS Evolved6-61

6.2 Future Testing of Different Jamming Solutions –Field and Lab6-61

Appendix A: US Frequency Bands & CIS Testbed Support..... A-1

Appendix B: Table of AcronymsB-1

LIST OF FIGURES

Figure 1-1 Overview of Elements of a Contraband Interdiction System	1-5
Figure 1-2 High-Level Project Timeline	1-7
Figure 1-3 Contraband Interdiction System Workshop Agenda	1-9
Figure 2-1 CIS Testbed High Level Block Diagram	2-14
Figure 2-2 CIS Testbed Lab Diagram	2-17
Figure 2-3 Example Cell Tower Map in Vicinity of a Prison.....	2-19
Figure 3-1 Example Output Power Spectrum of Jammer – Jamming Band 717-756 MHz; 0-6 GHz span ..3-28	
Figure 3-2 Cellular Network Surrounding Lee Correctional Institution	3-30
Figure 3-3: Indoor MAS Installation (antenna at left).....	3-31
Figure 3-4: Outdoor MAS Installation in "Dog Run"	3-31
Figure 3-5 Cellular Network Surrounding Mark W. Stiles Unit	3-32
Figure 3-6: MAS Indoor Access Node.....	3-33
Figure 3-7: MAS Outdoor Access Nodes	3-33
Figure 3-8 Lee Correctional Institution Walk Route.....	3-35
Figure 3-9 Mark W. Stiles Unit Walk Route.....	3-36
Figure 3-10 Lee Correctional Institution TEMS Script Execution Locations	3-37
Figure 3-11 Mark W. Stiles Unit TEMS Script Execution Locations	3-38
Figure 3-12 Lee Correctional Institution East Exterior Facility Entrance Aggregated Spectrum Readout (0-3 GHz).....	3-39
Figure 3-13 Mark W. Stiles Unit Uncovered North Corridor Aggregated Spectrum Readout (0-3 GHz) 3-39	
Figure 3-14 Lee Correctional Institution Housing Unit Recreational Yard Aggregated Spectrum Readout (0-3 GHz)	3-40
Figure 3-15 Mark W. Stiles Unit Housing Unit 12 Aggregated Spectrum Readout (0-3 GHz).....	3-40
Figure 3-16 Mark W. Stiles Unit Housing Unit 12 2.4 GHz Channel Spike (2-3 GHz)	3-41
Figure 3-17 Mark W. Stiles Unit Housing Unit 7 Recreational Yard 5.2 GHz Channel Spike (5-6 GHz)...	3-41
Figure 3-18 Lee Correctional Institution Northwest Exterior Perimeter 5.8 GHz Channel Spike (5.7-5.9 GHz).....	3-42
Figure 3-19 MAS Coverage for Provider 1.....	3-43
Figure 3-20 MAS Coverage for Provider 2.....	3-44
Figure 3-21: MAS Coverage for Provider 3	3-45
Figure 3-22: MAS Coverage for Provider 4	3-46
Figure 3-23: Contraband WiFi Hotspot in Dormitory.....	3-47
Figure 3-24: MAS Coverage throughout Mark W. Stiles Unit for Provider 1	3-48
Figure 3-25: MAS Coverage throughout Mark W. Stiles Unit for Provider 2	3-49
Figure 3-26: MAS Coverage throughout Mark W. Stiles Unit for Provider 3.....	3-50
Figure 3-27: MAS Coverage throughout Mark W. Stiles Unit for Provider 4.....	3-51
Figure 3-28: WiFi Hotspot in Housing Unit 7 at Mark W. Stiles Unit	3-52

1 INTRODUCTION

1.1 HISTORY & PURPOSE

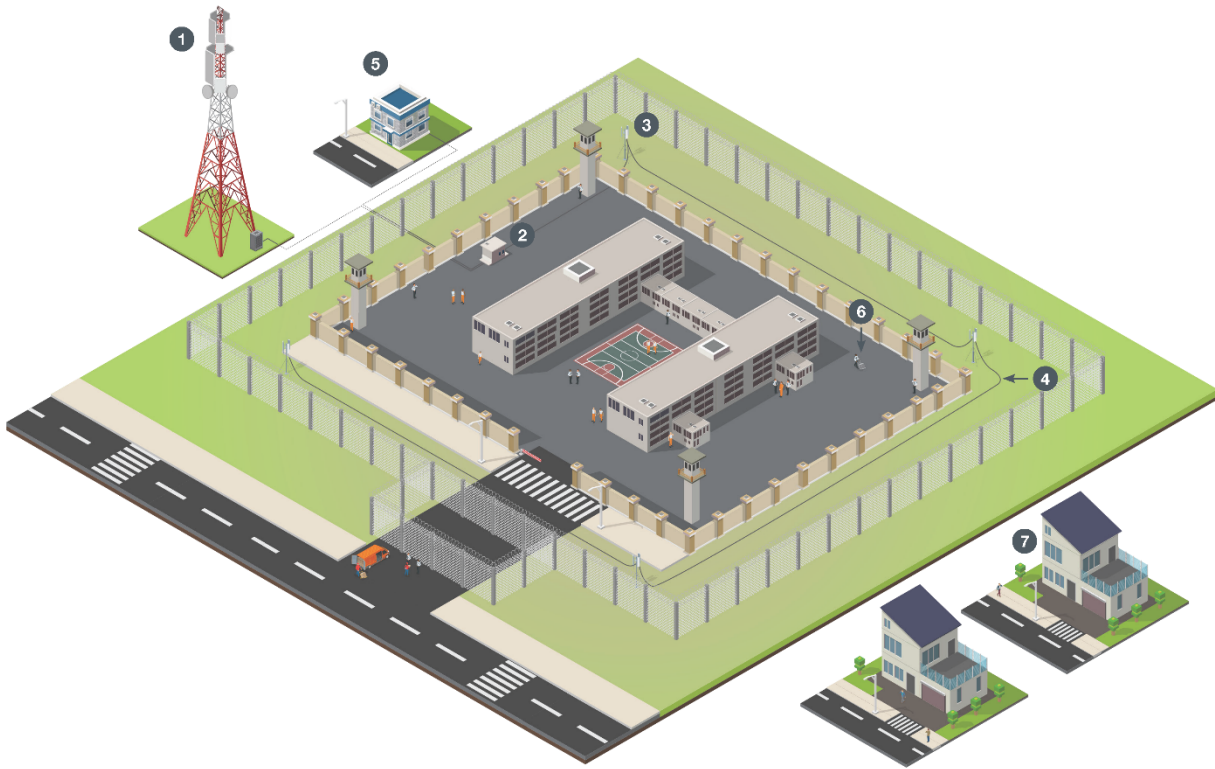
In February 2018, the Federal Communications Commission (FCC), under the leadership of Chairman Ajit Pai, convened a stakeholder meeting to discuss solutions to contraband cell phones in state correctional facilities. Chairman Pai explained the initiative’s goal as follows: “to bring together a diverse group to determine the most effective, affordable, and safe ways to address this problem—that is, to stop the threat of contraband cellphones without causing harm to legitimate wireless users.” In April 2018, CTIA and the Association of State Correctional Administrators (ASCA) launched the Contraband Phone Task Force.

Through the Task Force, CTIA and the wireless industry set out to work with the corrections community to establish a test bed to assess Contraband Interdiction System (CIS) technologies. CIS technologies are deployed in correctional facilities to combat use of unauthorized mobile phones, and their effectiveness in denying and/or detecting phones is a function of many parameters, including the radiofrequency (RF) environment, type and configuration of phones, and the characteristics of the commercial mobile networks operating in the area. CTIA and the wireless industry demonstrated their commitment to the Contraband Phone Task Force by funding the development and execution of the CIS Test Bed. CIS vendors contributed through their participation in the CIS Workshop and providing equipment, coordination, and collaboration for testing. Additionally the CIS vendors paid a fee to participate in the testbed.

This report summarizes the activities to test and evaluate CIS technologies and provides “best practice” recommendations on their use.

1.1.1 Contraband Interdiction Systems

CIS technologies are deployed in correctional facilities to combat use of unauthorized mobile phones, and their effectiveness in denying and/or detecting phones is a function of many parameters, including the RF environment, type and configuration of phones, and the characteristics of the commercial mobile networks operating in the area. An overview of elements that can be included in a CIS deployment is provided in the figure below.



Overview of a Contraband Interdiction System

Contraband Interdiction Systems (CIS) detect unauthorized user equipment (UE) and prevent unauthorized communications from escaping a correctional facility. Examples of CIS are Denial of Service Systems (DSS), Managed Access Systems (MAS), and Cell Detection Systems (CDS). CIS deployments are unique, complex installations with multiple components. Common elements of CIS are described below:

- | | |
|--|---|
| <p>1 Cell Tower</p> <ul style="list-style-type: none"> • Provides service to the macro network <p>2 CIS Control Hub</p> <ul style="list-style-type: none"> • Manages all CIS functions • Routes calls, SMS, and data from authorized UEs to the macro network • Blocks calls, SMS, and data from unauthorized UEs <p>3 CIS Antenna</p> <ul style="list-style-type: none"> • Creates RF perimeter around correctional facility • Captures all incoming RF emanations from Cell Towers surrounding correctional facility • Captures all outgoing RF emanations from UEs within correctional facility • Indoor and outdoor options | <p>4 Rigid Conduit</p> <ul style="list-style-type: none"> • Connects CIS Antennas to CIS Control Hub • Built to Law Enforcement Agency specifications to protect against sabotage <p>5 Public Safety Answering Point</p> <ul style="list-style-type: none"> • CIS routes 911 calls from all UEs to PSAP (configurable based on facility requirements) <p>6 Cell Detection System</p> <ul style="list-style-type: none"> • Conducts mobile, periodic sweeps of facility to detect contraband UEs <p>7 Neighborhood in Close Proximity to Correctional Facility</p> <ul style="list-style-type: none"> • Per 47 CFR § 1.9020(n), CIS vendors must notify general public 10 days prior to system activation |
|--|---|

Figure 1-1 Overview of Elements of a Contraband Interdiction System

1.1.2 Contraband Phones Task Force selection of CIS Testbed Administrator

Following-up on their commitment to the Task Force, the wireless industry selected Dr. Charles Clancy, , Bradley Professor of Cybersecurity, Electrical and Computer Engineering from Virginia Tech, and the Virginia Tech Applied Research Corporation (VT-ARC), to administer a testbed program that includes both laboratory testing and in-facility testing for CIS technologies. Dr. Clancy and a team from VT-ARC—Mr.

Mike DiFrancisco, Mr. Kristoffer Lemoins, and Mr. Adam Gorski—acted as the CIS Testbed Administrator for this project.

1.1.3 Summary of CIS Testbed Administrator Statement of Work

The CIS Testbed Administrator “Contraband Phone Project” 2018 Statement of Work (SOW) included the following tasks:

- Task 0 – Program Support
 - Coordination and engagement with CTIA and Contraband Phone Task Force members
 - Weekly calls with CTIA and CTIA members
 - Attend and lead all test bed-related presentations and discussions at Contraband Phone Task Force meetings
- Task 1 – Engagement and Scoping; May – July 2018
 - Plan and execute a 2-day vendor workshop on Contraband Interdiction Systems
 - Formulate a request for participation in the test bed from CIS vendors
 - Work with task force members to review and select candidate technologies for testing
 - Task 1 Deliverables:
 - Contraband Interdiction System Workshop – Coordination, Hosting and Materials
 - Final report: “CIS Workshop Vendor Summaries”
 - Added deliverable: Inputs to the “Call to Participate in the Contraband Interdiction System Testbed” disseminated to candidate vendors & evaluation of responses
- Task 2 – Laboratory Testing; July-October 2018
 - Acquire equipment based on the specified laboratory test plan and equipment specification & Integrate the CIS Testbed Laboratory
 - Perform per-vendor product/technology testing
 - Task 2 Deliverables:
 - Test Reports:
 - “Contraband Interdiction System (CIS) Laboratory Test Report – (*Jammer Vendor 1*) Jammer”
 - “Contraband Interdiction System (CIS) Laboratory Test Report – (*MAS Vendor 1*) MAS”
 - “Contraband Interdiction System (CIS) Laboratory Test Report – (*MAS Vendor 2*) MAS”
 - PowerPoint presentation summarizing test results: “CIS Technology Testbed Update for Contraband Phone Task Force”
 - Related Deliverable: “Contraband Interdiction System (CIS) Laboratory Design”
 - Related Deliverable: “Contraband Interdiction System (CIS) Test Plan”
- Task 3 – First Test Site; July-October 2018
 - Objective: Test multi-layer technologies within a rural correctional facility that has already deployed
 - Conduct a visit to the selected site (“Site Survey”); Acquire and engineer field testing equipment; Develop systematic field testing approach; Perform test
 - Task 3 Deliverables:
 - First Test Site Test Report: “Lee Correctional Institution Field Test Report”
- Task 4 – Second Test Site and Wrap Up; November – December 2018 (extended to January 2019)

- Objective: Test collection of non-MAS technologies in an urban setting to assess interference.
 - Note that this objective was revised due to the federal prohibition on operations of a jammer at a non-federal field site. A second MAS installation was evaluated.
- Conduct a visit to the selected site (“Site Survey”); Acquire and engineer field testing equipment; Perform test
- Author a best practices whitepaper that makes recommendations on how to best deploy CIS technologies into correctional facilities and deliver to the task force members
 - Note: This report includes those best practice recommendations
- Host a wrap up workshop to share results and lessons learned
 - Note: in conjunction with the ASCA 2019 Winter Conference, New Orleans LA, 10 January 2019
- Task 4 Deliverables:
 - Second Test Site Test Report: “Mark W. Stiles Unit Field Test Report”
 - Best Practices Whitepaper: “Contraband Interdiction System (CIS) Testbed Report – Best Practices” (this report)

The overall flow of the project is illustrated in the figure below.

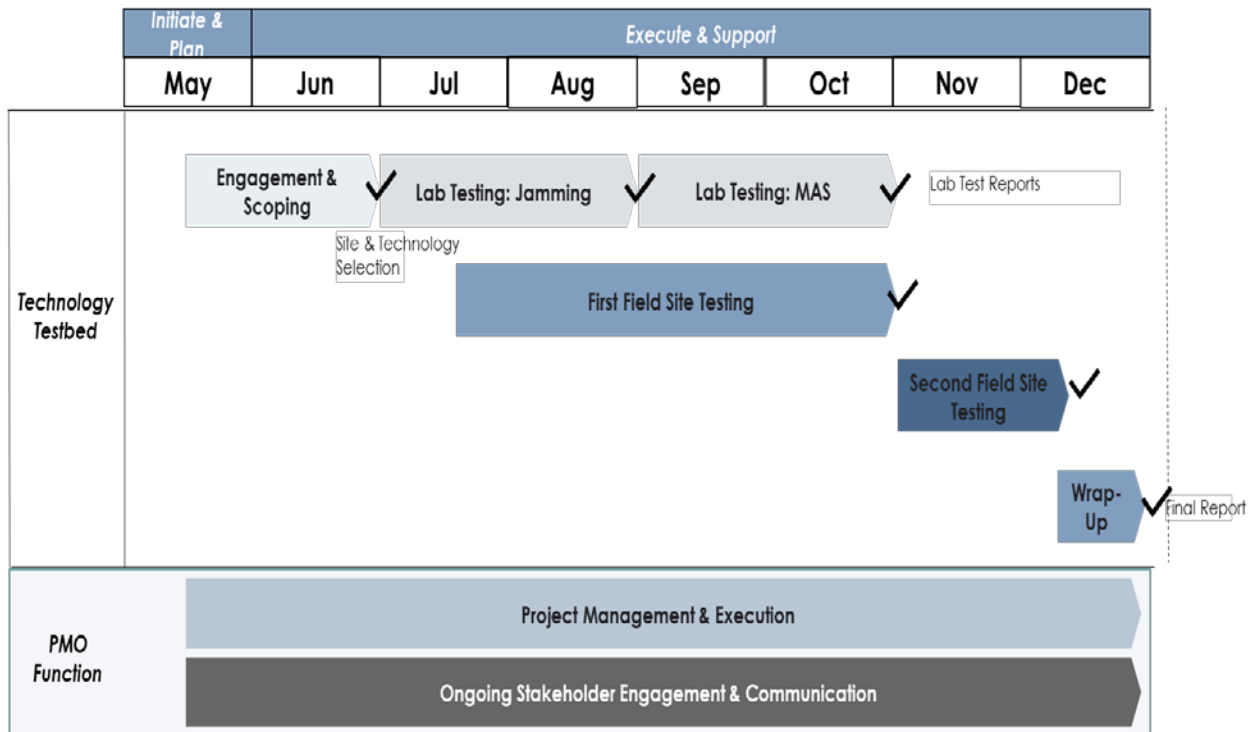


Figure 1-2 High-Level Project Timeline

1.2 ENGAGEMENT WITH CONTRABAND PHONE TASK FORCE

Coordination and engagement with CTIA and Contraband Phone Task Force members occurred through weekly calls, with CTIA and CTIA members and hosting/leading the CIS Workshop and participation at

Contraband Phone Task Force meetings. The CIS Testbed Administrator presented status and results on the CIS Testbed at each of these meetings, including:

- Contraband Interdiction System Workshop – 13-14 June 2018
 - CIS Technology Overview
 - Presentations from 12 CIS Solutions vendors
- Contraband Phone Task Force Meetings/Presentations
 - 30 April 2018, Washington DC
 - 14 June 2018, Arlington VA – After CIS Workshop
 - 7 September 2018, Arlington VA – Including CIS Testbed Tour/Demo
 - 10 January 2019, New Orleans LA – ASCA Winter Meeting

Regular interaction occurred with carriers through weekly calls, and preparations for field tests. The carriers provided details about their local cell coverage in the areas for each of the field tests.

Regular interactions were also held with corrections officials. The CIS Testbed Administrator requested, and ASCA provided, suggested field test locations. Additionally the Testbed team coordinated closely with officials from the states where testing was performed. Details of that coordination are described below under the CIS Testbed Field (Correctional Facility) Testing section.

1.3 OUTREACH AND ENGAGEMENT WITH CIS VENDORS

1.3.1 CIS Vendor Workshop

On 13-14 June 2018, the CIS Testbed Administrator hosted a “Contraband Interdiction System Workshop” in Arlington VA. During the workshop, Dr. Clancy presented a review of the potential CIS technologies and plans for testing and evaluation of these technologies in a laboratory managed by VT-ARC at the Virginia Tech Research Center, 900 N. Glebe Road, in Arlington. Eleven vendors of CIS technology presented overviews of their technologies. One additional vendor participated, but did not present.

June 13 – Day 1 Vendor Presentations

The Day 1 workshop provided an opportunity for CIS technology vendors to discuss their products and solutions.

June 14 – Day 2 Morning Agenda: MAS and Geofencing Sessions (9:00 AM – 12:00 PM)

Day 2, Session 1 – MAS (9:00 – 10:15)

Objective: Discuss challenges that correctional facilities have experienced in deploying MAS, with the goal of identifying approaches to remediate issues and increase reliability of the technology.

Day 2, Session 2 - Geofencing (10:30 – 12:00)

Objective: Identify opportunities and barriers in deploying a carrier geofencing solution within carrier networks.

June 14 – Afternoon: CIS Task Force Meeting (Task Force members only) (1:00 PM - 4:00 PM)

CONTRABAND INTERDICTION SYSTEM WORKSHOP

June 13-14, 2018 · Arlington, VA

June 13 - Day 1

8:00AM - 9:00AM	Registration and Breakfast outside of F Scott Fitzgerald E
9:00AM - 9:10AM	Welcome - Charles Clancy
9:10AM - 9:20AM	Wireless Industry Opening Remarks - CTIA
9:20AM - 9:30AM	Corrections Officials Opening Remarks - ASCA/BOP
9:30AM - 10:30AM	Testbed Program Overview - Charles Clancy
10:30AM - 11:00AM	Testbed Program Q&A - All Attendees
11:00AM - 12:00PM	Session I -CIS vendor presentations
12:00PM - 1:00PM	Lunch
1:00PM - 3:00PM	Session II -CIS vendor presentations
3:00PM - 3:15PM	Break
3:15PM - 4:00PM	Open Session for the Audience
4:00PM	Closing Remarks - Charles Clancy

June 14 - Day 2

8:30AM - 9:00AM	Registration and Breakfast outside of Ernest Hemingway 1 & 2
9:00AM	MAS Workshop - Clancy Introduction Technology Options Operational Experiences Best Practices Discussion
10:15AM	Break
10:30AM	Geofencing Workshop - Clancy Introduction Basic Approach Operationalization Regulatory and Standards Issues
12:00PM	Lunch
1:00PM - 4:00PM	Task Force Meeting - Contraband Phone Task Force Members from the Wireless Industry and Correctional Community ONLY



Figure 1-3 Contraband Interdiction System Workshop Agenda

1.3.2 CIS Workshop Vendors

- Securus Technologies - Wireless Containment Solution (WCS)
- Harris - CellDefender MAS solution
- ShawnTech - Hybrid MAS: CellDetect and CellInte
- Prelude Development - Geo-fencing
- CellAntenna - DAS systems
- Metrasens - Cellsense Ferromagnetic Phone Detection
- J3 Technologies - Shielded Micro Jammer Technology (SMJ)
- Tecore - iNAC (Intelligent Network Access Controller) MAS solution
- NCIC - Jammers
- Corrections.com – MAS
- SafeCell Technologies - Hybrid MAS
- Global Tel Link (GTL, did not present) - MAS

1.3.3 Vendor Participation in CIS Testbed

All of the vendors that participated in the CIS Workshop and several others were invited to participate in lab testing through a formal “Call to Participate”. Subsequently, four of those vendors (representing three CIS solutions – see table), accepted that invitation. The three solutions were tested during August and September 2018. (Note: Two companies (listed as Company A and Company B in the table below) that participated in the CIS Workshop responded separately to the Call to Participate, but tested as a single entity since they are teamed to provide a single MAS solution).

Table 1-1 CIS Testbed Participating Vendors

Company	Technology Type	Note
Company A	MAS	Agreed to joint lab testing. Supported testing of MAS installed at Mark W. Stiles Unit near Beaumont, TX. (a TX state prison)
Company B	MAS	
Company C	MAS	Agreed to lab testing. Supported testing of MAS installed at Lee Correctional Institution - location of first field test selected by ASCA
Company D	Jammer	Agreed to lab testing. Vendor was willing to provide additional jammer units for field test (field testing was not performed due to the federal prohibition on operations of a jammer at a non-federal field site)

2 CONTRABAND INTERDICTION SYSTEM TESTING PROCESS

Vendors for three CIS solutions volunteered to participate in testing: one jamming solution and two managed access systems (“MAS”). The CIS Testing Process involved lab testing and, where lawful, field testing. Lab testing evaluates systems under closely controlled conditions. Field testing sheds light on CIS performance in real-world conditions.

In July and August 2018, the CIS Testbed Administrator developed and integrated the “CIS Testbed” to evaluate CIS technologies in a controlled environment. The CIS Testbed Administrator also developed tools and techniques for performing tests of CIS solutions deployed in prison environments. The CIS Testbed Administrator implemented this testing regime to help better understand the performance of different types of technologies and how they can be synthesized in order to effectively combat contraband phones, while also managing the inadvertent impact they have on commercial mobile network subscribers in the vicinity of correctional facilities.

CIS vendors that have their technologies tested by the CIS Testbed received a copy of the test report that details their measured performance across a range of different scenarios. Separate reports were prepared for Field Testing at correctional facilities. These reports may be shared with Task Force members under a restricted dissemination, and were used to formulate a best practices guide that can be broadly shared with the corrections industry.³

2.1 CIS TESTBED LABORATORY TESTING

This section provides a description of the CIS Testbed and test plans and procedures. Summary results of testing are provided in the next section.

- **Objective:** Laboratory testing of different CIS technologies and products to assess effectiveness in repeatable, controlled scenarios
- **Approach:** Inclusive and transparent, allowing vendors to provide products and participate for a nominal testing fee
- **Implementation:** Laboratory testbed architecture based on use of small cells (vendor: ip.access Limited) operating with each of the key cellular technologies
 - Provide test reports to vendors
 - Aggregate information used to develop public best practices guide for CIS deployments

2.1.1 Context: Taxonomy of Contraband Interdiction Systems

This section includes taxonomy of CIS devices. This taxonomy of devices determines the applicability of certain types of testing.

³ See Executive Summary and *Section 5, Suggested Guidelines and Best Practices* for a best practices guide.

2.1.1.1 Denial of Service Systems (DSS)

A Denial of Service System (DSS) is a device or system of devices that is designed to prevent mobile phones from operating in a localized region. A subclass of devices, known as jammers, introduces interference into the uplink and/or downlink spectrum bands to prevent signaling between phones and base stations. Another subclass of devices, known as a cell site simulator (CSS), attracts phones into attaching and prevents them from effectively making calls.

2.1.1.2 Managed Access System (MAS)

A Managed Access System (MAS) is a deployment of active base stations within an operational facility, combined with a whitelist/blacklist feature set that prevents unauthorized calls. A MAS may be deployed using a Distributed Antenna System (DAS), or through a network of small cells. The MAS may interface with commercial cellular infrastructure to allow whitelisted and emergency phone calls to be properly routed.

2.1.1.3 Cell Detection System (CDS)

A Cell Detection System (CDS) is designed to detect and often localize phones in the environment. It may use passive (CDS-P) techniques or active techniques (CDS-A).

A CDS-P is an RF analyzer that is able to receive the uplink and downlink RF spectrum and identify any activity within those bands that indicates the presence of an unauthorized phone. These systems may be deployed persistently, potentially with the ability for multiple devices to cooperate in localizing phones; or could be used for periodic, mobile sweeps and include a direction-finding capability to localize unauthorized phones.

A CDS-A is a CSS that is able to not only identify the presence of a mobile device, but also other unique identifiers such as its IMSI and IMEI. A CDS-A is most commonly used for periodic, mobile sweeps.

No CDS system vendors applied for testing.

2.1.2 Test Plan – Systematic Lab Testing Approach

This section defines the overall test plan. Each test refers to the CIS technology under test (“TECHNOLOGY”), the laboratory testbed detailed in 2.1.3 Testbed Architecture, the small cells that represent the commercial cellular network (“NETWORK”), and the devices that represent the contraband phones (“PHONE”).

2.1.2.1 Band Support

Applicability DSS, MAS, CDS-P, CDS-A

Purpose US mobile carriers provide service over a range of frequencies. In order to be effective, the TECHNOLOGY must be able to support all frequencies that are within use by operators in the region.

Procedure Assess which of the bands listed in Appendix A are supported by the TECHNOLOGY and produce a summary as part of the test report that identifies band support.

2.1.2.2 Transmission and Spectral Mask

Applicability DSS, MAS, CDS-A

Purpose Adjacent channel interference can have a major impact on services operating in the vicinity of the TECHNOLOGY. This test will evaluate this interference.

Procedure Capture and document the spectral mask for the TECHNOLOGY when it is operating at its highest power level, for each of its configured frequency bands.

2.1.2.3 RF Denial Performance Test

Applicability DSS, MAS

Purpose The effectiveness of a PHONE is a function of the relative energy from the NETWORK and the TECHNOLOGY. This test will explore the RF denial effectiveness as a function of relative power in the LAB.

Procedure Use the LAB to assess the denial performance of the TECHNOLOGY as a function of relative signal strengths.

2.1.2.4 RF Detection Performance

Applicability CDS-P, CDS-A

Purpose The ability for the TECHNOLOGY to detect a PHONE is a function of the relative signal strength between the TECHNOLOGY, PHONE, and NETWORK. This test will explore detection performance as a function of relative power in the LAB.

Procedure Use the LAB to assess the detection performance of the TECHNOLOGY as a function of relative signal strengths. (Note: since no CDS systems were provided, this test was not performed).

2.1.2.5 Countermeasure Configuration

Applicability DSS, MAS, CDS-P, CDS-A

Purpose Different combinations of PHONE band support, NETWORK band support, or PHONE cell selection configuration may impact whether a particular TECHNOLOGY is effective. This test seeks to identify if there are any PHONE configurations that may allow the TECHNOLOGY to be ineffective.

Procedure Use the LAB to explore different PHONE configurations that may allow that PHONE to bypass the TECHNOLOGY.

2.1.2.6 Physical Security

Applicability DSS, MAS, CDS-A, CDS-P

Purpose The TECHNOLOGY will likely be deployed into more exposed locations within the operational environment. This test will assess how difficult it would be to disable them through physical attack.

Procedure Execute a sequence of non-destructive tests to assess the resilience of the device while it is connected to the LAB.

2.1.3 Testbed Architecture

This section describes the CIS Testbed architecture. The CIS Testbed is designed in such a way to support testing a diverse set of CIS devices to assess their performance in detecting and blocking use of cell phones. The purpose is to not necessarily create a realistic environment, but rather a controllable and repeatable environment where technologies can be tested in a rigorous manner and results compared across different devices in a meaningful way.

The CIS Testbed laboratory is focused only on CIS technologies that interact with a cell phone’s wireless interfaces. It does not seek to test other forms of detection. Specifically the CIS testbed is designed to support testing of jammers and other denial of service-type devices, Managed Access Systems (MAS), and cell detection systems like IMSI catchers.

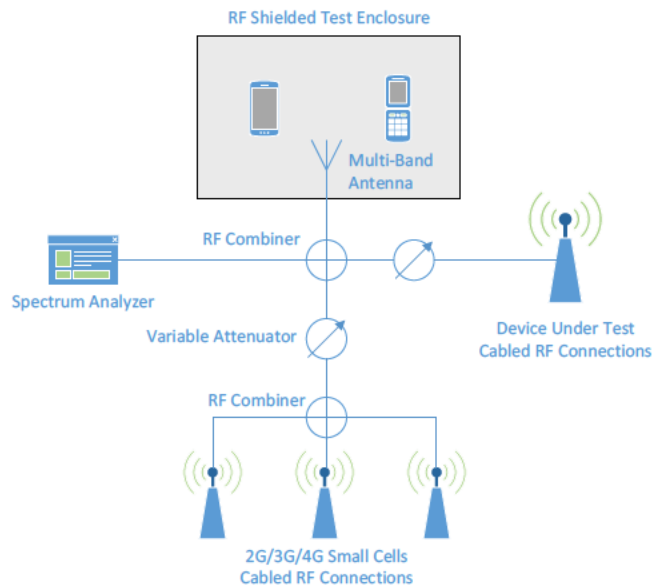


Figure 2-1 CIS Testbed High Level Block Diagram

2.1.3.1 Channel Emulator

The channel emulator consists of analog RF components that are used to connect together the various components of the testbed and simulate different channel conditions.

The RF shielded enclosure is a Ramsey STE3000 featuring RF connectors and shielded power. It contains an HG72703MGURB-SM multiband antenna able to communicate across the various relevant cell bands from 700 MHz to 2.4 GHz. This antenna provides connectivity to PHONES that are housed within the shielded enclosure.

For testing requiring more interactive engagement with devices, VT-ARC used an RF shielded room. When strict control of relative power levels is not required, devices can operate over the air within the RF shielded room.

A programmable, four-channel variable attenuator (RC4DAT-6G-95) is a key feature of the channel test network. It allows devices within the network to be connected at a range of different relative power levels. It is connected to a laptop that is used to control the attenuation settings between the PHONE and the NETWORK and between the PHONE and TECHNOLOGY.

The channel emulator also includes a range of different cables and fixed attenuators used to connect together the different components and appropriately calibrate the needed RF power levels.

2.1.3.2 Cell Network Emulator

To emulate the cell network, a solution from ip.access was integrated to support synthesis of the macro cell network signaling. The system is based around a software-based cellular core network developed by

Druid, and resold by ip.access. The system has support for both 2G/3G core network and 4G core network functions. The cell network emulator equipment was procured with licenses allowing it to support Short Message Service (SMS) and Voice over LTE (VoLTE) services to support a wide range of testing needs.

With respect to the radio access network (RAN), several base stations were integrated into the system. These include:

- GSM Edge 850 MHz small cell (CLR)
- GSM Edge 1900 MHz small cell (PCS)
- Nano3G S8 small cell – configured for UMTS band 2/5 (PCS, CLR)
- S60 LTE small cell – configured for LTE band 2 (PCS)
- S60Z UMTS/LTE small cell – reconfigurable to support 625-2800 MHz and 3300-3800 MHz

Support for LTE SMH (700 MHz) and AWS (1700 MHz) bands was accomplished via the reconfigurable S60Z module which through software can be tuned to support many different frequency bands. This module also supports both FDD and TDD operation, so TDD operation in BRS/EBS (2500 MHz) and CBRS (3500 MHz) can also be tested.

2.1.3.3 Test Phones

Phones are required to interact with the technologies and within the testbed.

Correctional facility officials from multiple jurisdictions provided actual interdicted phones from correctional facilities in order to help ensure that the testing is motivated by the types of phones commonly seen in correctional facility environments. While these phones provide ground truth about the types of contraband devices found in correctional facilities, many are locked to specific carriers or have other access controls that make their use in the testbed more difficult.

The CIS Testbed Administrator procured a collection of unlocked phones that represent the types of devices represented by those provided from correctional facilities. The collection includes both easily hidden miniature phones, like the LONG-CZ T3, and also an assortment of commonly available phones found in any retail store.

In order to interact with the NETWORK, SIM/UIM cards are needed that have encryption keys provisioned into the ip.access system. The ip.access acquisition included 30 test SIMs that were pre-provisioned to operate with the test network.

2.1.3.4 Measurement Equipment

A collection of other measurement equipment is also being integrated into the laboratory.

The Testbed includes a PCTEL SeeGull IBflex (<https://www.pctel.com/scanning-receivers/>). This device scans the cellular frequencies and can provide a detailed breakdown of base station signaling and power levels. It was used to help diagnose and understand how different devices and systems in the testbed are interacting with each other, and will also be a key asset in later field testing.

In addition to equipment procured under the CTIA-funded contract, the VT-ARC lab also includes other equipment used in the CIS Testbed, including a set of diagnostic UEs (cell phones) called TEMS (from

InfoVista) and a Wavejudge 5000 Wireless Test System (from Sanjole). The TEMS devices are used to record discrete interactions between the UE and the network. TEMS Discovery software is used for analysis. The Sanjole Wavejudge device is able to monitor LTE control channel traffic by decoding the RF uplink and downlink control channels.

The tables below list the CIS Testbed Equipment procured under this project:

Table 2-1 CIS Testbed Channel Emulator Equipment

Device	Description	Qt
RC4DAT-6G-95	Programmable Variable Attenuator, 4 ch	1
VAT-10+	Fixed Attenuator 10 dB	20
FL086-6SM+	Interconnect Cables SMA	20
ZVA-183W+	Wideband LNA	1
ZN4PD1-63HP-S+	RF Combiners (4 way)	4
HG72703MGURB-SM	Multiband Cell Antenna	8
501-1035-ND	RF adapter kit	2
STE3000	RF test enclosure	1
PCTEL SeeGull IBflex	RF cellular measurement	1

Table 2-2 CIS Testbed Network Emulation (ip.access) Equipment

Device	Description	Qt
470-Z-04-U32	S60Z reconfigurable NB/eNB	1
435-R-04-U32	S60 eNB	1
237BA	S8 NB	1
165DU	GSM EDGE BTS 850	1
165H	GSM EDGE BTS 1900	1
ABASW-30-234G	Lab Softcore (Druid) 2G/3G/4G, VoLTE, SMS	1

The figure below diagrams the interconnection of the equipment in the CIS Testbed laboratory.

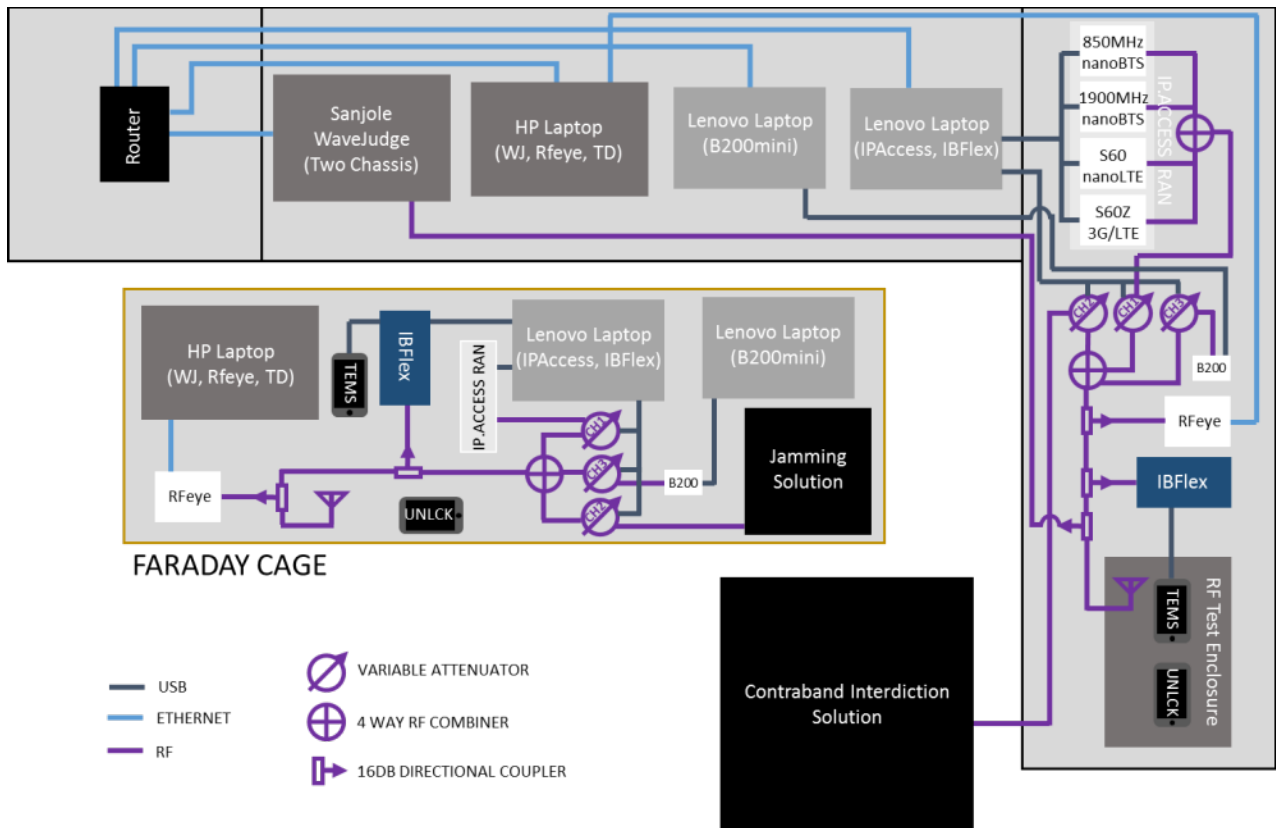


Figure 2-2 CIS Testbed Lab Diagram

2.2 CIS TESTBED FIELD (CORRECTIONAL FACILITY) TESTING

This section provides a description of the CIS Testbed and test plans and procedures. Summary results of testing are provided in the next section.

- **Objective:** Test multi-layer technologies within a rural correctional facility that has already deployed a CIS
- **Approach:** Learn real-world issues and deployments of MAS in order to better understand how the systems function and provide recommendations
- **Implementation:** Conduct detailed site survey and test visit in a variety of locations throughout the facility; run scripts on UEs to stress MAS
 - Provide test reports to correctional facilities and MAS vendors
 - Aggregate information used to develop public best practices guide for CIS deployments

2.2.1 Field Testing Approach

The overall approach for field testing includes the following steps:

- Identify Required Field Test Equipment
- Coordinate with Wireless Carriers to get information about local cells
- Coordinate with Prison Officials & Installed CIS Vendors
- Organize and Execute a Site Survey

- Perform Field Test

2.2.2 Field Test Equipment

Detailed data collection was carried out using the following set of equipment.

Hardware:

- PCTel IBFlex Scanning Receiver – channel seeking blind scanning, RAT power measurement, LTE layer 3 messaging
- CRFS RFeye Node Receiver – spectrum analyzer
- 4 TEMS test UEs (one per carrier: ATT, Sprint, T-Mobile, Verizon) – RAT and WiFi power measurement*, scripting of various RAT capabilities

Software:

- PCTel SeeHawk Collect – companion software to IBFlex
- CRFS RFeye Site – spectrum analysis companion software to RFeye Node
- TEMS Pocket – test UE interface for data collection and scripting
- TEMS Discovery – post processing software allowing for deep analysis of collected TEMS Pocket data.

*NOTE: Neither of the MAS that were tested in the field were required to interdict the use of contraband cell phones operating WiFi hotspots, or connecting to such hotspots. The equipment used for testing allowed the Testbed team to perform these measurements without any additional steps and so it was included in the testing. The results illustrate a use of contraband phones that would otherwise have been unknown.

2.2.3 Coordination with Wireless Carriers

Before data collection a survey of local carrier towers was performed. This consisted of driving around the vicinities of all nearby carrier towers and taking power (RSRP) measurements using all four TEMS test phones. This allowed for confirmation of tower asset ownership and colocation on a carrier basis.

- Tower Location (latitude - longitude, address)
- For each Radio Access Technology at that location:
 - Band
 - Center Frequency (UL & DL)
 - Bandwidth
 - antenna height
 - antenna azimuth pointing direction
 - antenna downtilt
 - cell/sector identifier: e.g., PCI, PN, PSC, CID (function of RAT)



Figure 2-3 Example Cell Tower Map in Vicinity of a Prison

2.2.4 Coordination with Correctional Facility & Vendor

The CIS Testbed Administrator coordinated with representatives from the prisons, and the CIS Vendor to review Site Survey objectives. Teleconferences were scheduled to ensure logistics for the visits were planned and a successful visit could be achieved.

2.2.5 Site Survey

Site Survey Objectives:

- Familiarization with the facility, its operations, and operating procedures
- Detailed discussion on the cellular interdiction issues specific to the facility, to include understanding how devices enter the facility, are used within the facility, and are discovered within the facility
- Detailed discussion with the IT staff and MAS support engineer about the MAS deployment
- Detailed discussion on detected use of phones in the facility and any inferences that can be drawn on limitations of the MAS based on interdicted phones and/or detected uses
- Walkthrough within the correctional facility doing a preliminary cellular RAN signal surveys, using a diagnostic equipment to record MAS & cell tower identities and power levels
- Drive around the correctional facility perimeter (outside the outer fence) doing the same survey
- Drive test on public roadways within a 10km perimeter of the correctional facility doing the same survey

Example Site Survey Agenda:

- 8:00: Testbed Administrator Team Arrives at Correctional Facility
- 8:30 - 10:30: Meet in Conference Room

- Overview of Correctional Facility & Security Briefing
- Summary of CIS Test plan & Site Survey plan – CIS Administrator Team
- MAS Overview presentation – MAS Vendor
- 10:30 – 11:00: Tour MAS Vendor Equipment Installation
- 11:00-12:00: Meet in Conference Room
 - Detailed discussion of correctional facility & MAS network
- 12:00 – 1:00: Lunch (officers dining hall)
- 1:00 – 2:30: Signal Surveys Inside Correctional facility – Walk through several residence units & outdoors inside fence line (loosely cover the entire range of buildings and yards)
- 2:30-3:30: Initial Findings Summary in Conference Room; Determine date for final testing
Adjourned ~ 3:30

Site Survey Measurements:

The CIS Testbed Team used cellular testing equipment and a portable Spectrum Analyzer to measure carrier and MAS signals within and beyond correctional facility boundary:

- PC Tel SeeGull IBflex Scanning Receiver with SeeHawk Collect software
 - “Blind” scan to determine all cell signals received at selected locations
 - Layer 3 decoding on selected identified signals
- TEMS Diagnostic UE interaction with carrier (& MAS) Networks
 - 4 TEMS devices with SIMs/accounts on each of major network providers: AT&T, Sprint, T-Mobile, Verizon
 - Plotted (contraband-based - TBD) WiFi signals
 - Data evaluated using TEMS Discovery software
- CRFS RFEye Spectrum Analyzer
 - Power Spectral Density plots at various locations in and outside of correctional facility

Data was analyzed in the field, and evaluated in detail after the Site Survey using TEMS Discovery software. A Field Test Plan was developed based on results of the Site Survey.

Before data collection began a signal survey of local carrier towers was performed. This consists of driving around the vicinities of all nearby carrier towers and taking power (e.g., Reference Signal Receive Power - RSRP) measurements using TEMS test phones with service plans on each of the four wireless carriers. This allowed for confirmation of tower asset ownership and colocation on a carrier basis.

2.2.6 Field Test Event

Detailed data collection was carried out by the CIS Testbed Team using cellular testing equipment and a portable spectrum analyzer to measure carrier and MAS signals within and beyond correctional facility boundary.

Hardware:

- PCTel IBflex Scanning Receiver – channel seeking blind scanning, RAT power measurement, LTE layer 3 messaging
- CRFS RFEye Node Receiver – spectrum analyzer

- 4 TEMS test UEs (one per carrier: ATT, Sprint, T-Mobile, Verizon) – RAT and WiFi power measurement, scripting of various RAT capabilities

Software:

- PCTel SeeHawk Collect – companion software to IBflex
- CRFS RFeye Site – spectrum analysis companion software to RFeye Node
- TEMS Pocket – test UE interface for data collection and scripting
- TEMS Discovery – post processing software allowing for deep analysis of collected TEMS Pocket data.

Testing included measurements performed inside the correctional facility according to a walk route that the Testbed team pre-coordinated with the correctional facility officials, along with a slow drive around the perimeter of the correctional facility. During the perimeter drive the team performed a blind scan using the IBflex scanner. The purpose of this scan was to determine channels present in the immediate vicinity of the correctional facility. Example scan data showing detected technologies and associated channels is provided in the table below.

Table 2-3 Example PCTel Blind Scan Detected Channels



Throughout the exterior perimeter ride spectrum data was collected with the RFeye, while power and WiFi scans were conducted with the four TEMS test UEs.

To achieve the highest level of data diversity during interior testing a walk route was formulated. This walk route included various locations of interest that would detail the effects of building shadowing and indoor/outdoor environment on the MAS.

Data collection on the interior of the correctional facility was carried out using the IBflex scanner, RFeye Node, and the four TEMS test UEs. During the initial walkthrough the IBflex Scanner and RFeye Node

were rolled on a cart, taking continuous measurements throughout the entirety of the walk route. The TEMS test UEs were carried in a notebook, taking continuous power and WiFi scan measurements.

A second walkthrough was performed with the TEMS test UEs running a 20-minute script in various locations throughout the correctional facility. The TEMS scripts attempted to replicate a contraband phone's ability to use voice, data, and text services throughout the facility. The script was developed to emulate a human attempt to try and escape the MAS through repeated attempts to send text messages, attempt voice calls, and access data services.

The TEMS script consisted of the following steps:



The TEMS script was executed in multiple locations within each facility.

3 CIS TESTBED RESULTS SUMMARY

This section provides the results of lab testing and field testing for three systems: Two MAS (lab and field test for each) and one jammer (lab test only).

3.1 MAS LAB RESULTS SUMMARY

Two MAS solutions were tested in the lab.

Each MAS consisted of multiple software defined radios (SDRs) tuned to the tester’s choice of bands. MAS #1 was fully functional, possessing the same capabilities as the vendor’s deployed MAS unit, except for bypassing the final RF stage. It supported GSM, UMTS, LTE FDD, and LTE TDD bands. All test bands were supported. Harmonics were present for some of the bands tested and it was determined these harmonics would have been filtered out by the final RF stage. Along with contraband interdiction functionality, MAS #1 had whitelisting, 911 dialing, whitelisted mobile to mobile calling, and blacklisted data session redirection capabilities. All additional capabilities were successfully demonstrated in the lab. MAS #2 was a stripped down version of the vendor’s deployed MAS unit for compatibility with the limited laboratory space and power. MAS #2 supported GSM, UMTS, and LTE FDD. LTE TDD was not supported in the tested configuration. MAS #2 included filters for the most common GSM, UMTS, and LTE bands.

The tested MAS network configuration is for deployments where roaming agreements are not implemented. In this case, the MAS will force the contraband cell phone to step down to a 2G service where authentication is not required. In this configuration, the RF emitted requires enough signal to noise ratio above the macro network to confuse a contraband UE into thinking there is no other network available. Both MAS had this configuration available during the ongoing testing.

Results Summary

The two MAS solutions succeeded in blocking communications from contraband devices over simulated and actual cellular networks. The effectiveness of the MAS solutions depended on the power of the interdiction systems’ signals relative to the surrounding commercial cellular networks, as well as their coverage of frequency channels used by contraband devices. In its laboratory testing, VT-ARC incrementally decreased the power of the MAS networks until test devices attached to the simulated cellular network, revealing a “crossover” point at which actual contraband phones would evade interdiction.

Band Support Test Results

In both configurations, RF emissions must ensure unintended emanations are not produced from the MAS. Four band combinations were chosen for testing against each MAS:

- GSM 850; UMTS 2; LTE 4
- GSM 850; UMTS 2; LTE 12
- GSM 1900; UMTS 5; LTE 13
- GSM 1900; UMTS 5; LTE 17

As MAS #1 supported LTE TDD, two additional band combinations were tested against it.

- GSM 1900; UMTS 5; LTE 41
- UMTS 5; LTE 2; LTE 41

Transmission & Spectral Mask

Detailed plots of RF emissions across all the supported bands are included in the Appendix C of the Test Reports entitled, “Contraband Interdiction System (CIS) Laboratory Test Report – (MAS Vendors A/B & C) MAS”.

During testing, harmonics and emissions in other RF bands were present at times for MAS #1. It was determined that these harmonics would have been filtered out by the final RF stage that was bypassed in the lab to obtain compatible power with the laboratory system. These harmonics did not affect system performance.

RF Denial Performance Test

Six of the lab’s test phones supported all chosen bands. All test phones were Android smartphones. Test phones with non-Android operating systems were omitted because the contraband phones received from prisons (over 50 separate devices) included NO iOS devices (iPhones/iPads). This does not present a limitation because all devices (Android, iOS, etc.) satisfy the same standardized Radio Access Network interface requirements that are the focus of the CIS Testbed evaluation. Note that omitting iOS devices allowed the use of a less expensive wireless diagnostic application: Network Cell Info Lite.

Baseline signal strength was established for each band and technology before denial performance testing was carried out. The lab attenuator was used to position the network signal strength lower than the MAS signal strength. MAS #1 vendor specified a signal strength difference of 6-10dB for all technologies. A difference of 9dB was used for testing. When testing MAS #2 the following power levels were adhered to:

- For LTE bands a difference of 9dB used
- For UMTS a difference of 6 dB used
- For GSM a difference of 3dB used

Once baseline power levels were established, home network signal level measurements were taken at strong (0dB home network attenuation), medium (15dB home network attenuation), and weak (30dB home network attenuation) cell strength levels. The MAS was then turned on. MAS attach success was indicated and resulting signal strength was recorded. If the test phone attached to the MAS the MAS was attenuated in 1dB increments until a crossover to the home network was observed. Crossover signal strength and channel were recorded. This test process was repeated for the remaining 5 test phones. Measurements were then repeated for all remaining band combinations. Specific cross-over points for each configuration are documented in the lab test reports.

Countermeasure Configuration




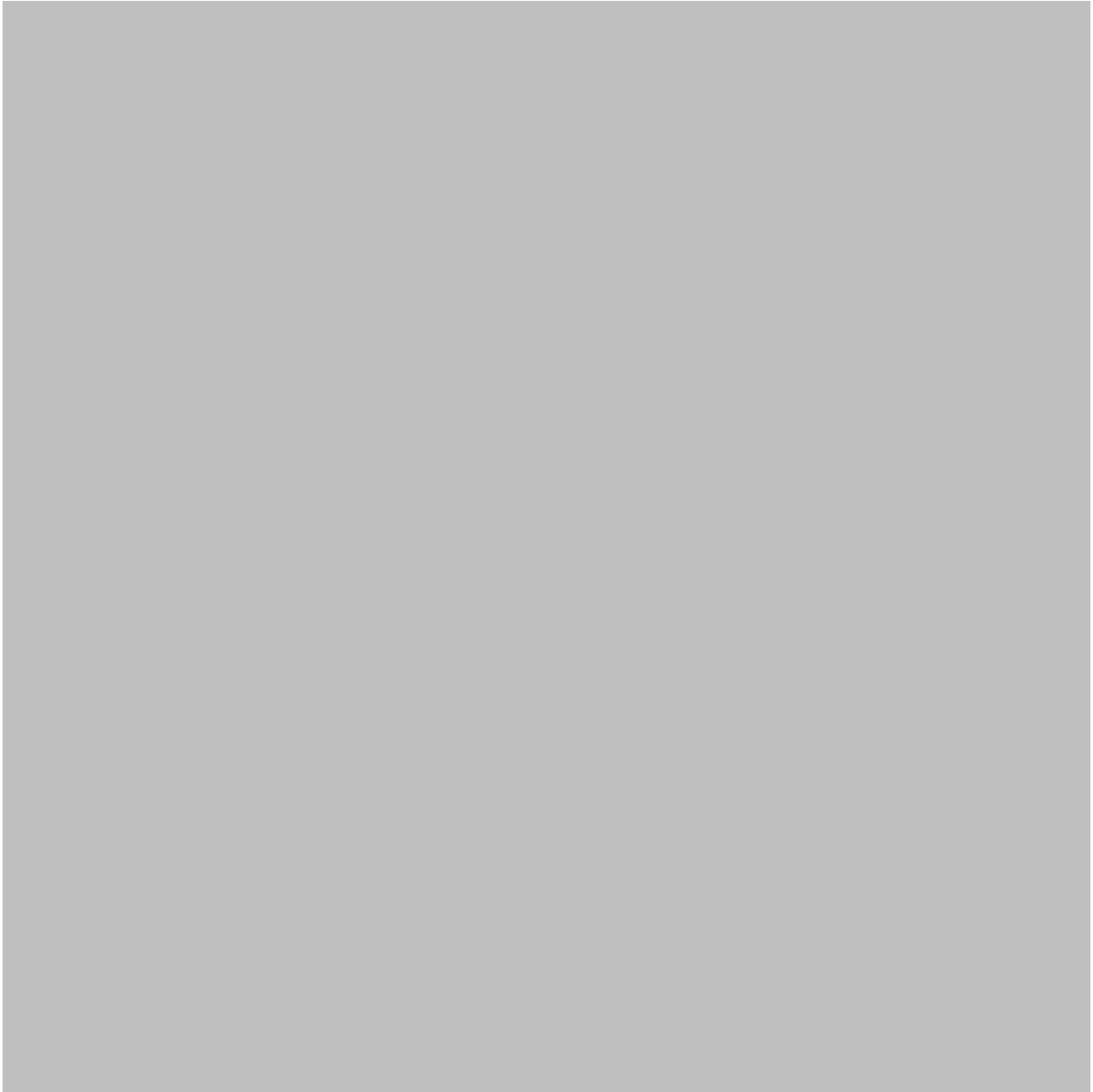


Physical Security

The assessment in this section is based on evaluation of MAS documentation, and interviews with MAS vendors and correctional facility personnel.

Each MAS consists of several subsystems when fielded:

- A main primary hub which contains the network switching equipment, MAS core network, and remote connectivity system;
 - Secondary hubs which control various sectors of the facility to which the MAS is fielded; and
 - Remote units which interface with external antennas
- 



3.2 DSS (JAMMING) LAB RESULTS SUMMARY

One jamming solution was tested in the lab.

- 5-channel jammer unit
 - 717-756 MHz
 - 851-896 MHz
 - 1930-1995 MHz
 - 2110-2200 MHz
 - 2350-2360 MHz

Results Summary

- Denial of service independent of Radio Access Technology
- The jammer successfully denied performance to the UE once the network signal level was overshadowed by the jamming channel
- Only countermeasure is introducing non-jammed frequency or disabling jamming functionality
- Multitude of harmonic channels emitted (1-8 per jamming channel) representing significant out of band interference to other channels.

Only one of four devices from the vendor was tested because the other three devices were not operating properly: The output power was not controlled by the front panel knobs as intended. These devices could not be controlled to represent accurate results.

Table 3-1 Specified frequency bands and power levels for tested jammer

Frequency Channel	Power Rating
717-756 MHz	3W
851-896 MHz	3W
1930-1995 MHz	2W
2110-2200 MHz	2W
2350-2360 MHz	2W

Notable Events

During our testing of one of the units the power supply shorted out on the night of 10 September 2018. This caused the test to be postponed until a new power supply was acquired.

At the same time of the power supply short it was discovered that the other unit (a six channel version) output power was not controlled by the front panel knobs as intended; despite all outputs being terminated and all knobs in the off position the unit still generated power out. This discovery was confirmed using the RFEye spectrum analyzer with receive antenna, and further testing with the unit was terminated due to expectation that results would not be accurate or meaningful.

Band Support Test Results

The CIS Testbed is configured to support for testing of all 2G, 3G, and 4G (both FDD and TDD) technologies, in a subset of bands, including LTE bands: 2, 4, 10, 12, 13, 17, but not 29, 66, 71, 252, 255.

The jammers that were delivered are capable of downlink jamming in all the evaluated bands with the exception of 5GHz TDD bands.

Transmission and Spectral Mask

Spectral masks were captured of all jamming outputs on the unit. It was found that the in-channel radiated power for a specific frequency channel is far from the 3W specified figure. Values were found to be 0.05 mW or less for each frequency channel, with adjacent channels occurring with each of the 6 jamming ports. A large portion of the jammer’s emanated RF energy is transmitted as wideband noise, raising the ambient noise floor by as much as 30 dB. Spectral masks show a minimum of 1 and

maximum of 8 adjacent channels. Results were very similar with the second tested unit however power output per port was >20dB less. The reason for the disparity is unknown.

Detailed measurement values at each port of the two devices. Example power spectrum plots from the spectrum analyzer are shown below.⁴

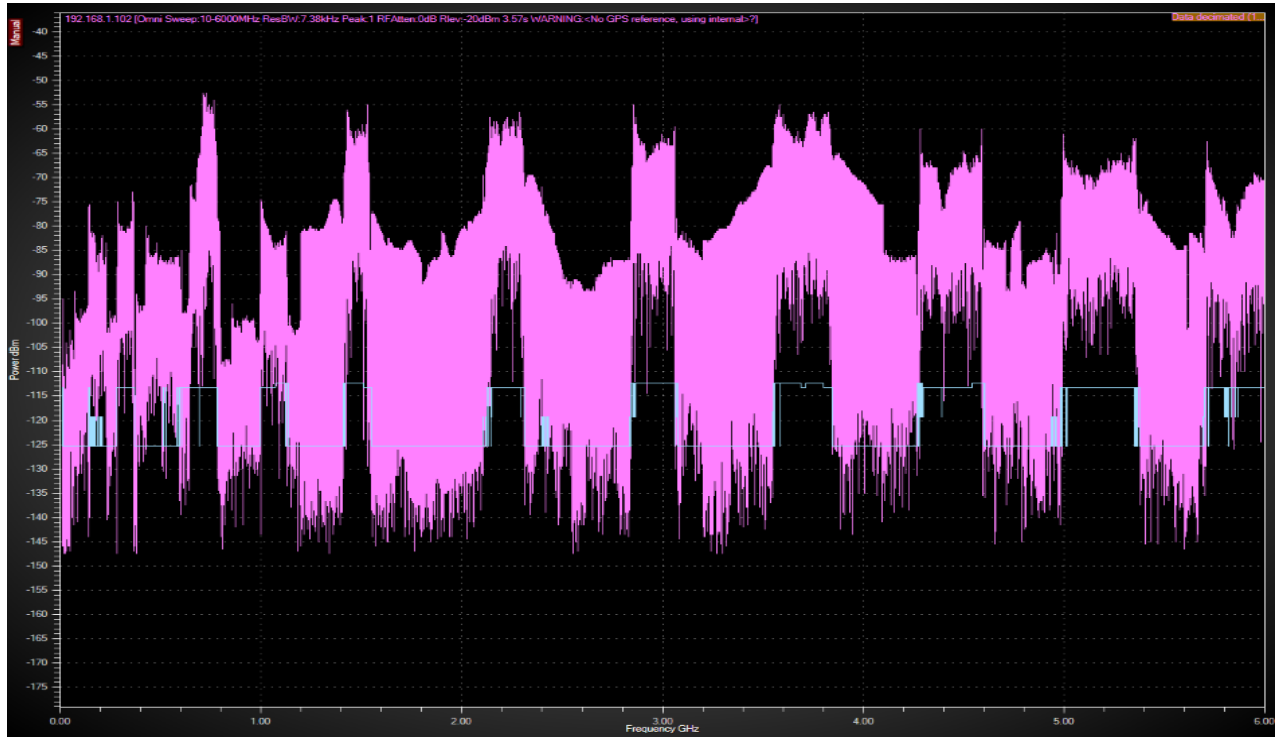


Figure 3-1 Example Output Power Spectrum of Jammer – Jamming Band 717-756 MHz; 0-6 GHz span

RF Denial Performance Test

RF denial performance was tested using the ip.access private wireless network. Each jamming channel was tested with corresponding 2G/3G/4G technology bands. A test phone with corresponding band support was connected to the un-attenuated network while the jammer was off. Measurements of signal strength and DL/UL throughput were taken. The network was then attenuated in 10dB steps, with signal strength and DL/UL throughput measurements recorded at each step. This process was repeated twice, once with the jammer at half power knob position, then again with the jammer at full power knob position. Once measurements were made for all three jammer settings, the entire process was repeated for the next jammed test channel.

This part of testing was only carried out with one of the provided jammer units, as it was deemed the only jammer that did not exhibit RF leakage when powered on.

⁴ Detailed plots for every port across all the specified bands are included in the Appendix C and Appendix D of the Test Report entitled, “Contraband Interdiction System (CIS) Laboratory Test Report – (Jammer Vendor 1) Jammer.”

In the jammer off knob position behavior of the UEs was normal, with throughput corresponding to technology used. Network connectivity remained present until high levels of attenuation were introduced.

Because knob position and power level were not uniform among the five jammer channels, variances in necessary network attenuation were present in the jammer half power knob position. As network attenuation increased both signal strength and throughput decreased. Throughput measurements became impossible after a certain signal threshold was crossed, resulting in signal strength data extending into further attenuation settings.

In the jammer full power knob position data throughput was never present at 10+ dB attenuation. The jammer successfully denied performance to the UE once the network signal level was overshadowed by the jamming channel.

In four out of five tested LTE bands the UE mistakenly recognized the more powerful jammer channel as the network channel, resulting in high signal strength numbers despite high levels of network attenuation.

Countermeasure Configuration



Physical Security





3.3 MAS FIELD TEST RESULTS SUMMARY

Two facilities were visited for MAS field testing: Lee Correctional Institution in Bishopville, South Carolina, and Mark W. Stiles Unit in Beaumont, Texas.

Lee Correctional Institution MAS Overview

Lee Correctional Institution deploys a MAS to prevent unauthorized and contraband cellular devices from communicating with macro cellular networks across all four major providers. Lee Correctional Institution has 11 cellular towers in a five mile radius of the facility that provide coverage from AT&T (under lease from Farmers Telephone Cooperative, Inc.), Sprint, T-Mobile, and Verizon. There is no tower reuse in the immediate vicinity of the facility; all of the towers in the area only contain antennas from one cellular provider.



Figure 3-2 Cellular Network Surrounding Lee Correctional Institution

The MAS at Lee Correctional Institution consists of three key components to function:

- RF planning and infrastructure deployment throughout the facility to create a “radio frequency umbrella” that fully covers the Lee facility;
- Allow / block lists for approved / unauthorized user equipment (UE), respectively; and
- Continued management of RF systems, maintenance of MAS, and continual RF planning to optimize the system.

The MAS is installed in several locations throughout Lee to provide optimal coverage and block cell phones from unauthorized users from accessing the macro network. The system is paired with a distributed antenna system and contains two types of radio frequency nodes:

- Internal nodes for indoor coverage of inmate accessible buildings and dormitories
- External nodes for outdoor coverage of recreational yards and lawns

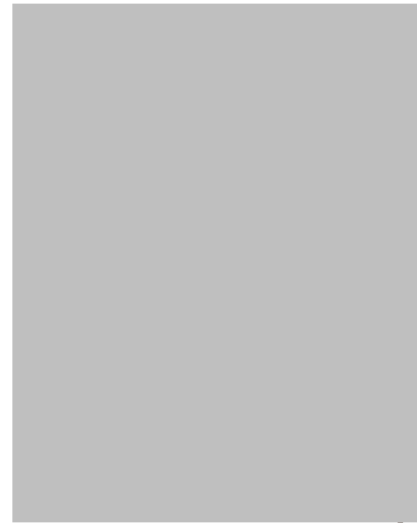


Figure 3-3: Indoor MAS Installation (antenna at left)

Internal nodes consist of ruggedized antenna housings attached to walls or ceilings throughout the facility. External nodes consist of similar ruggedized antenna housings; however, they are attached to masts and predominantly located within the facility’s “dog run” (i.e., the rock-filled and razor-wire lined area between perimeter fencing) or mounted to the roofs of buildings. The nodes are connected via RF-over-fiber to RF hubs located throughout the facility and finally to a centralized hub within the administration building. All areas are access controlled and built to South Carolina Department of Corrections (SCDC) specifications for resilience to damage from weather and inmate sabotage.

The Lee MAS consists of multiple software defined radios (SDRs) to cover and manage the RF macro environment within Lee Correctional Institution. The SDRs can be provisioned as required to assist with new macro channels, adjust power levels, and survey for changes to the macro network. The system is configured to route all 911 calls to the Lee Correctional Institution watch office. This office is the same location that any landline 911 call would go to in an emergency. Contraband phone users have the ability to call 911 and contact this office; any other dialed number will connect to a MAS service that plays a recorded message stating that the UE is contraband, its identifying information and call data has been logged, and then disconnects the call. Data services are redirected to a webpage that shows similar information as a voice call. There are no roaming agreements with the macro providers; therefore, any UE 3G / 4G services are blocked, the connection is stepped down to 2G, and terminated according to the process described above.



Figure 3-4: Outdoor MAS Installation in “Dog Run”

The Lee MAS is wholly run by vendor engineers. Limited SCDC personnel have access to the vendor technology, its functionality, and reporting capabilities. The vendor provides daily activity reports to SCDC via e-mail to provide information on cell phone restrictions, inmate communications, and other data as requested. There is a remote troubleshooting and monitoring interface that the vendor utilizes to manage the system via VPN; a full-time vendor engineer is responsible for operation and continued maintenance of the hardware and software aspects of the system.

Mark W. Stiles Unit MAS Overview

Mark W. Stiles Unit deploys a MAS to prevent unauthorized and contraband cell phones from communicating with macro cellular networks across all four major providers. The unit has 16 cellular towers in the vicinity of the facility that provides coverage from AT&T, Sprint, T-Mobile, and Verizon. The cellular network primary serves the nearby communities of Beaumont and Nederland, Texas; thus there are several instances of tower re-use in the immediate vicinity of Stiles.



Figure 3-5 Cellular Network Surrounding Mark W. Stiles Unit

The current Stiles MAS is the second deployment of a cell phone blocking system at Stiles. The first deployment of a cell phone blocking system was deployed by a different vendor and was restricted to 2G and 3G systems. The current MAS vendor was contracted to augment the existing system, install 4G services, and further optimize the MAS system at Stiles to ensure optimal coverage within the facility.



The Stiles MAS consists of three key components to function:

- RF planning and infrastructure deployment throughout the facility to create “fence to fence” control throughout the facility
- Allow / block lists for approved / unauthorized user equipment (UE), respectively; and
- Continued management of RF systems, maintenance of MAS, and continual RF planning to optimize the system

The MAS at Mark W. Stiles Unit is paired with a distributed antenna system and contains two types of radio frequency nodes:

- Internal nodes for indoor coverage of inmate accessible buildings and dormitories
- External nodes for outdoor coverage of recreational yards, lawns, and external pathways between buildings



Figure 3-6: MAS Indoor Access Node



The Stiles MAS consists of multiple software defined radios (SDRs) to cover and manage the RF macro environment within Mark W. Stiles Unit. The SDRs can be provisioned as required to assist with new macro channels, adjust power levels, and survey for changes to the macro network. The system is configured to route all 911 calls to the local Public Safety Answering Point (PSAP) in Jefferson County, Texas. This office is the same location that any landline 911 call would go to in an emergency. Emergency 911 calls routed through the MAS include a pseudo number and provide the dispatcher with a location of Mark W. Stiles Unit for emergency response. Contraband phone users have the ability to call 911 and contact this office; any other dialed number will immediately disconnect the call after relevant information on the UE has been logged. Data services are redirected to a webpage that shows the user has accessed a blocked website. There are no roaming agreements with the macro providers; therefore, any UE 3G / 4G services are blocked, the connection is stepped down to 2G, and terminated according to the process described above.



Figure 3-7: MAS Outdoor Access Nodes

The Stiles MAS is wholly run by vendor engineers. Limited TDCJ personnel have access to the MAS technology, its functionality, and reporting capabilities. The vendor provides daily activity reports to TDCJ and provides information on allow / block listing, cell phone

restrictions, inmate communications, and other data as requested. There is a remote troubleshooting and monitoring interface that the vendor utilizes to manage the system via VPN.

MAS Field Testing Execution & Results

At both facilities detailed data collection was carried out using the following set of equipment.

Hardware:

- PCTel IBflex Scanning Receiver – channel seeking blind scanning, RAT power measurement, LTE layer 3 messaging
- CRFS RFeye Node Receiver – spectrum analyzer
- 4 TEMS test UEs (one per carrier: ATT, Sprint, T-Mobile, Verizon) – RAT and WiFi power measurement*, scripting of various RAT capabilities

Software:

- PCTel SeeHawk Collect – companion software to IBflex
- CRFS RFeye Site – spectrum analysis companion software to RFeye Node
- TEMS Pocket – test UE interface for data collection and scripting
- TEMS Discovery – post processing software allowing for deep analysis of collected TEMS Pocket data.

*NOTE: Neither of the MAS that were tested in the field were required to interdict the use of contraband cell phones operating WiFi hotspots, or connecting to such hotspots. The equipment used for testing allowed the Testbed team to perform these measurements without any additional steps and so it was included in the testing. The results illustrate a use of contraband phones that would otherwise have been unknown.

Before data collection at each facility began a survey of local carrier towers was done. This consisted of driving around the vicinities of all nearby carrier towers and taking power (RSRP) measurements using all four TEMS test phones. A few photos of the towers were taken as well. This allowed for confirmation of tower asset ownership and colocation on a carrier basis.

Upon arrival at the facility the testing team drove around the exterior perimeter. During this drive a blind scan was carried out using the IBflex scanner. The purpose of this scan was to determine channels present in the immediate vicinity of the facility. Throughout the exterior perimeter ride spectrum data was collected with the RFeye, while power and WiFi scans were conducted with the four TEMS test UEs.

In order to achieve the highest level of data diversity during interior testing a walk route was formulated. This walk route included various locations of interest that would detail the effects of building shadowing and indoor/outdoor environment on the MAS.



Figure 3-8 Lee Correctional Institution Walk Route



Figure 3-9 Mark W. Stiles Unit Walk Route

Data collection on the interior of the correctional facility was carried out using the IBflex scanner, RFeye Node, and the four TEMS test UEs. During the initial walkthrough the IBflex Scanner and RFeye Node were rolled on a cart, taking continuous measurements throughout the entirety of the walk route. The TEMS test UEs were carried in a notebook, taking continuous power and WiFi scan measurements.

A second walkthrough was carried out with the TEMS test UEs in which a 20-minute script was run in various locations throughout the correctional facility. The TEMS scripts attempted to replicate a contraband phone's ability to use voice, data, and text services throughout the facility. The script was developed to closely emulate a human attempt to try and escape the MAS through repeated attempts to send text messages, attempt voice calls, and access data services.

The TEMS script consisted of the following steps:





The TEMS script was carried out in various locations within the facilities, as seen in the figures below.



Figure 3-10 Lee Correctional Institution TEMS Script Execution Locations



Figure 3-11 Mark W. Stiles Unit TEMS Script Execution Locations

Spectrum readouts cannot distinguish between MAS network signal versus carrier network signal.





Figure 3-12 Lee Correctional Institution East Exterior Facility Entrance Aggregated Spectrum Readout (0-3 GHz)



Figure 3-13 Mark W. Stiles Unit Uncovered North Corridor Aggregated Spectrum Readout (0-3 GHz)

Figures below show locations at Lee and Stiles where MAS coverage was known to be high. In these cases the aggregated spectrum readout picks up the high powered MAS antennas.



Figure 3-14 Lee Correctional Institution Housing Unit Recreational Yard Aggregated Spectrum Readout (0-3 GHz)



Figure 3-15 Mark W. Stiles Unit Housing Unit 12 Aggregated Spectrum Readout (0-3 GHz)



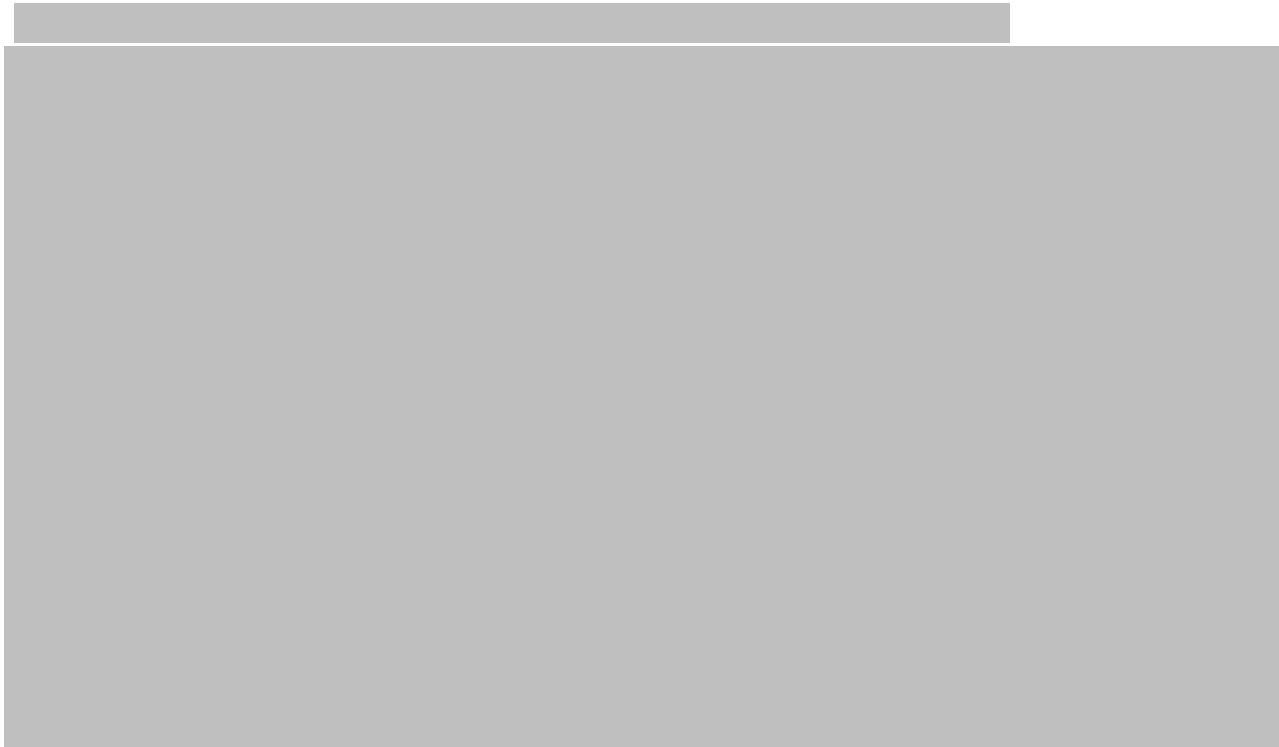


Figure 3-16 Mark W. Stiles Unit Housing Unit 12 2.4 GHz Channel Spike (2-3 GHz)



Figure 3-17 Mark W. Stiles Unit Housing Unit 7 Recreational Yard 5.2 GHz Channel Spike (5-6 GHz)

An instance of a 5.8 GHz channel spike is detected at Lee Correctional Institution at the northwest exterior perimeter, adjacent to the restricted housing units. This spike corresponds to WiFi 802.11 a/n channels. A weaker power reading relative to the 2.4 GHz spike can be explained due to distance from the adjacent housing unit.



Figure 3-18 Lee Correctional Institution Northwest Exterior Perimeter 5.8 GHz Channel Spike (5.7-5.9 GHz)

TEMS Phone sweeps were conducted throughout the Lee facility and consisted of a perimeter drive and interior walkthroughs. All four major cellular providers—ATT, Sprint, T-Mobile, and Verizon—were tested. Below are results from each of the walkthrough tests. Each cellular provider has been given a unique provider number and are not named in the below results.

Lee Correctional Institution is served by nine cellular towers and provides a challenging RF environment for the MAS. There are three cellular towers that provide a direct RF emanation over the Lee facility and provide strong coverage to the southern portion of the correctional facility.

Provider 1 deploys LTE coverage throughout the entire region and consists of three cellular towers surrounding the correctional facility.

[Redacted text block]

On the perimeter road, the MAS provided excellent containment of RF emissions. Within the Restricted Housing Unit (RHU), the system provided excellent coverage and prevented all communications.

On charts 3-19 to 3-22 below the colors represent the following:

- Green: Macro network service

- Yellow / Red: MAS network service: UE Receives warning messages; UE monitored and logged



Figure 3-19 MAS Coverage for Provider 1

Provider 2 deploys LTE coverage throughout the entire region and is served from one cellular tower approximately 1.5 kilometers west of the correctional facility. The MAS was successful at blocking unauthorized communications from within the facility in the required covered areas. [REDACTED]

[REDACTED] On the perimeter road, the MAS does leak coverage outside of the core facility; however, this is due to the antennas being very close to the road along the perimeter fencing. Within the Restricted Housing Unit (RHU), the system provided excellent coverage and prevented all communications.



Figure 3-20 MAS Coverage for Provider 2

Provider 3 deploys strong 3G and LTE coverage throughout the entire region and is served from five cellular towers surrounding the correctional facility. The MAS had several challenges with blocking unauthorized communications from within the facility in the required covered areas. Vendor engineers were aware of this situation and stated in August the cause was due to a recent re-provisioning of the network.



On the perimeter road, macro coverage was maintained, showing excellent RF containment from the MAS. Within the Restricted Housing Unit (RHU), the system provided excellent coverage and prevented all communications.



Figure 3-21: MAS Coverage for Provider 3

Provider 4 deploys LTE coverage throughout the entire region and is served from two cellular towers surrounding the correctional facility. One cellular tower is approximately 1.5 kilometers to the southeast of the facility and provides a direct RF line-of-sight beam over the southern portion of the facility. The MAS was successful at blocking unauthorized communications from within the facility in the covered areas. In one quarter of the facility, the TEMS phone reported LTE service; however, no calls were permitted. It appears the TEMS phone was erroneously reporting LTE service because it was locking onto an LTE band that was already covered by the MAS. [REDACTED]

[REDACTED] On the perimeter road, the MAS does leak coverage outside of the core facility; however, this is due to the antennas being very close to the road along the perimeter fencing. Within the Restricted Housing Unit (RHU), the system provided excellent coverage and prevented all communications.



Figure 3-22: MAS Coverage for Provider 4

The TEMS phones were configured to scan for contraband WiFi hotspots. Multiple hotspots were found on both visits to the facility. These hotspots can enable unauthorized internal communications within the correctional facility. Several can be located to dormitory areas within the facility. An example of this is shown below in Figure 3-23.



Figure 3-23: Contraband WiFi Hotspot in Dormitory

TEMS Phone sweeps were conducted throughout the Stiles facility and consisted of a perimeter drive and interior walkthroughs. All four major cellular providers—ATT, Sprint, T-Mobile, and Verizon—were tested. In each instance, the MAS blocked all call, data, and SMS attempts in areas where the system provided coverage. Below are results from each of the walkthrough tests. Each cellular provider number at Stiles is consistent with the cellular provider number at Lee.

Provider 1 deploys LTE coverage throughout the entire region and consists of six cellular towers surrounding the correctional facility. RF propagation from a nearby cellular tower approximately four kilometers to the east affects the RF environment in the vicinity of the correctional facility. The antenna directly pointing at the facility has created higher RF power at the southeast portion of the facility.

Nevertheless, the MAS was successful at blocking unauthorized communications from within the facility in the required covered areas. A “fringe area,” i.e., an area that was in a non-accessible area for inmates, was tested to evaluate the MAS at areas of weaker coverage due to close proximity to strong overhead RF emanations from the macro network. This was to gain additional information on how MAS operate in general and was not intended as a test case to attempt to defeat the MAS. In this case, the calls continued to be blocked and no communications were able to access the macro network. On the perimeter road, macro network services to Provider 1 were fully accessible, implying excellent containment of the RF from the MAS.



Figure 3-24: MAS Coverage throughout Mark W. Stiles Unit for Provider 1

Provider 2 deploys LTE coverage throughout the entire region and consists of three cellular towers surrounding the correctional facility. The towers are farther from the facility; therefore, the signal strengths from this provider are weaker than those found from Provider 1.

The MAS was successful at blocking unauthorized communications from within the facility in the required covered areas. During testing the TEMS phone for Provider 2 reported LTE coverage; however, no calls, SMS, or data services were granted to the phone. Upon discussions with vendor engineers we learned that the TEMS phone was erroneously reporting LTE services. The TEMS phone was actually attaching to other RF bands already covered on the MAS system in an attempt to find service. The MAS was blocking these services as well. On the perimeter road, macro network services to Provider 2 were fully accessible, implying excellent containment of the RF from the MAS.



Figure 3-25: MAS Coverage throughout Mark W. Stiles Unit for Provider 2

Provider 3 deploys LTE coverage throughout the entire region and consists of three cellular towers surrounding the correctional facility. The towers are farther from the facility than those of provider 1; therefore, the signal strengths from this provider are similar to those found from Provider 2. LTE coverage is degraded in the southwest portion of the facility, resulting in the phone to step down to UMTS coverage.

The MAS was successful at blocking unauthorized communications from within the facility in the required covered areas. [REDACTED]

[REDACTED] On the perimeter road, the cellular service continually stepped down from LTE to UMTS and there were two locations without service. The cause for this is unknown.



Figure 3-26: MAS Coverage throughout Mark W. Stiles Unit for Provider 3

Provider 4 deploys LTE coverage throughout the entire region and consists of seven cellular towers surrounding the correctional facility. One antenna directly pointing at the facility has created higher RF power at the eastern portion of the facility.

Nevertheless, the MAS was successful at blocking unauthorized communications from within the facility in the required covered areas. On the perimeter road, macro network services to Provider 4 were fully accessible, implying excellent containment of the RF from the MAS.



Figure 3-27: MAS Coverage throughout Mark W. Stiles Unit for Provider 4

In addition to cellular traffic, the TEMS phones were configured to scan for contraband WiFi hotspots. Medical equipment inside the infirmary was excluded from the scans. One SSID was identified during the November 1 scan of Housing Unit 7, shown in Figure 3-28. Upon return in October, this hotspot could not be found on a second WiFi scan attempt.



Figure 3-28: WiFi Hotspot in Housing Unit 7 at Mark W. Stiles Unit

4 SUMMARY OF FINDINGS

Summary of Lab & Field Test Results

Test	DSS/Jammer	MAS
RF Denial Mechanism	<ul style="list-style-type: none"> Compresses dynamic range of RF channel of phone until denial of service occurs; RF interference overcomes downlink signal synchronization 	<ul style="list-style-type: none"> Forces handset to step down to 2G where services are blocked MAS can handle or block LTE / UMTS services without step down; requires carrier roaming agreement (not available in field tests)
RF Denial Performance - Laboratory	<ul style="list-style-type: none"> Achieved: Dependent on relative power of desired signal Significant out of band interference present 	<ul style="list-style-type: none"> Achieved: Dependent on relative power of desired signal Substantial feature sets providing information and services to correctional facility officials
RF Denial Performance - Field	<ul style="list-style-type: none"> N/A - Field test not performed due to 47 U.S.C. § 333 and FCC policy prohibition on non-federal jammer operations 	<ul style="list-style-type: none"> Effective: MAS installed at two large state correctional facilities demonstrated effective control of contraband phone communications RF coverage design critical to effectiveness Key features demonstrated (911, allow lists, etc.)

4.1 MAS SOLUTIONS FINDINGS

Two MAS vendors volunteered to participate in testing. Both vendors participated in lab testing. Both vendors have existing MAS installations. Field testing of the first vendor’s MAS solution was coordinated with the South Carolina Department of Corrections (SCDC) and carried out on site at Lee Correctional Institution in Bishopville, SC. Field testing of the second vendor’s existing MAS was coordinated with the Texas Department of Criminal Justice and carried out on site at Mark W. Stiles Unit in Beaumont, TX.

Overall the MAS systems are effective in denying contraband phone access to cellular networks. In its field tests, VT-ARC observed that both MAS solutions were successful in blocking unauthorized communications in areas that the correctional facilities required to be covered. In addition, signals from both MAS solutions were contained within the correctional facilities, suggesting that the systems posed little risk of interference to legitimate wireless users beyond the facilities’ perimeters at the time of testing.

Potential Disruption of Carrier Networks/Recommendations to minimize spectrum interference:

Careful design of the RF distribution network is required to ensure MAS deployments do not disrupt customers on carrier networks. At Lee Correctional Institution, instances of local users in Bishopville, SC having their phones “captured” by the MAS were reported. In this case the MAS vendor was notified and adjusted the MAS to prevent future occurrences. This example highlights the need for careful RF design and routine monitoring of MAS signal levels relative to carrier network levels both inside and

outside the prison. Spectrum interference can be minimized using a DAS system with many antennas transmitting at relatively low signal levels with directivity away from the outside areas of the prison, along with careful and repeated measurement and monitoring.

Cost effectiveness:

MAS systems are a proven solution to the problem of contraband cell phone use in correctional facilities, and although the costs are not trivial, the CIS Testbed Administrator knows of no other technical solution that is as effective. Many correctional facilities have deployed MAS systems, although they may or may not be affordable for some correctional facilities.

MAS deployments require significant up-front investment; it follows that vendors require multi-year service contracts to recoup these up-front costs. One of the prisons tested was on its second MAS deployment, with some officials indicating that the first did not achieve its intended function of contraband interdiction. In these cases a vendor takes on a significant amount of risk if its MAS deployment is not in use for the entire duration of its service contract. In order to guarantee successful contraband interdiction, as well as minimization of disruption to carrier cellular networks, the system must be serviced and supported throughout its lifecycle.

In addition to denying contraband phone access to cellular networks, MAS systems include feature sets that are capable of providing information and services to correctional facility officials, including documentation of each specific instance where a contraband phone attempted to communicate.

Short or long term solution/Scalability:

Both MAS deployments visited showed a high level of effectiveness in contraband interdiction, however due to the systems' reliance on a 2G network stepdown, longevity of the system will be in question once manufacturers start rolling out cell phones without 2G capability (since carriers are already starting to move away from providing 2G services). Once that occurs, MAS vendors will need roaming agreements with carriers. We hypothesize that due to added complexity associated with incorporating the necessary interfaces required for roaming agreements, there may be some additional costs for MAS deployments. However, we also hypothesize that there may be substantial savings to be gained in minimizing the complexity of the RF distribution network for the MAS.

In any event, current MAS designs (at least the ones tested) must be considered "mid-term" solutions since their design approach is based on 2G technology. Note, however that many elements of the design, including the DAS and RF distribution network and much of the RAN hardware and software, could be reused in a solution designed for 3G & 4G roaming.

As 5G systems are deployed, MAS solutions operating at higher frequencies may be needed, if and when carrier deployments at these frequencies overlap with prison facilities at those locations, necessitating substantial redesign of the RF distribution network. (Note that this would be true for any CIS solution, including DSS & CDS.)

In the Stiles MAS deployment, hundreds of antennas are used to ensure accurate directionality of the MAS network. This level of effort may need to be replicated at any future MAS deployment in order for contraband interdiction success. Costs for RF distribution for the MAS solutions like those that were

tested generally are not amortizable over subsequent MAS deployments, as each prison offers its own unique RF challenges. (Other MAS design approaches addressed in the next steps section might serve to address this expense.)

System automation:

Once a MAS deployment is built, maintenance and service contracts will necessitate vendor support. MAS field tests informed the team that MAS-related technical issues cannot be addressed through automation in most cases. Due to the ever-changing spectral environment at a given prison, support must exist throughout the lifecycle of the MAS. In the case of a new cellular channel appearing in the vicinity of a prison, licensing requirements may preclude the automation of adding a new MAS channel on the fly.

4.2 DSS (JAMMING) SOLUTIONS FINDINGS

The CIS Testbed only received voluntary participation from one Jammer technology vendor. One other jammer technology vendor participated in the CIS Workshop, but chose not to participate in lab testing despite the solicitation to participate. While the initial VT-ARC project plan included the potential to field test a jamming DSS solution in a prison setting, 47 U.S.C. § 333 and FCC policy bar non-federal operations of jammers that interfere with radio communications of any licensed or authorized stations. This constraint prevented field testing of jammers during the duration of the Test Bed.

Potential Disruption of Carrier Networks/Recommendations to minimize spectrum interference:

Laboratory testing of one manufacturer’s jammer indicated a strong risk of generating substantial aggregate interference, both in the designed cellular bands, and out of band. This risk multiplies when multiple jammer units are used in a correctional facility deployment. Harmful interference to multiple communications domains (e.g., commercial cellular services, terrestrial communications including public safety, satellite communications, aviation, etc.) outside a correctional facility could occur.

The jamming solution that was tested in the CIS Testbed was not necessarily representative of all possible jammers that may be considered for use in U.S. correctional facilities. Testing additional jamming solutions in both laboratory and field conditions would be needed to more fully assess the likelihood of harmful interference.

Cost effectiveness:

For any jammer installation paramount importance is placed in the prevention of harmful interference to commercial services outside of a prison. While field testing was not conducted on the participating vendor’s jammers, it can be theorized that cost will be proportional to the complexity of the prison’s RF environment. For location-specific contraband prevention to work many jammers with fixed antennas, or a DAS-like RF distribution system would be needed, especially in the case of prisons in urban geographies. The complexity of such a deployment may result in costs approaching MAS installations.

Short or long term solution:

On-going maintenance and service is a must with any CIS installation – including jammers. Jammer vendors and correctional facility customers must account for future cellular band additions (including those for 5G high band cell systems, when deployed), and for any architectural changes that can reduce efficacy of the jammer system.

Similar to MAS solutions, as 5G systems are deployed, jammers operating at higher frequencies may be needed, and substantial redesign of the RF distribution network also may be necessary.

Scalability:

Jammer solutions that were presented at the CIS Workshop, and included in testing, are designed to be self-contained systems requiring only power to operate, but many individual jammers are required to cover a correctional facility – up to one jammer per inmate cell. This solution thus is simple to scale (assuming power is available everywhere), but the cost is linear with the floor area covered.

System automation:

Jammer designs of the type tested are inherently basic and not automated. This means that prison operators have nothing to adjust or interface to once jammers are deployed. However, it also means that there is no way to respond to new cell bands being deployed, except to deploy new jammer equipment, and there is no way to provide any cellular communications users to an “allowed list” (e.g., public safety officials).

5 SUGGESTED GUIDELINES AND BEST PRACTICES

5.1 MAS SOLUTIONS GUIDELINES AND BEST PRACTICES

Overall, MAS systems are effective in denying contraband phone access to cellular networks. The effectiveness is dependent on the relative power of desired signals, which is dependent on the MAS RF distribution network design. MAS require complex installations and long-term maintenance. At installation, significant planning must be performed to ensure the RF emanations from the MAS deployment do not interfere with the macro network or inadvertently block authorized communications. The system must continually adapt to issues due to the cellular environment, inmate activities, law enforcement agency requests, and concerns raised by the general public. MAS deployments present issues not only for the MAS itself, but also for the macro network, since the MAS identifies and blocks cellular providers’ RF emanations. Macro network emanations must be continually monitored in order for the MAS to be proactive against contraband communications and function at peak efficiency.

Issues with operation of a MAS system can be separated into three general categories:

- RF Deployment (RF)
- Maintenance (M)
- Interference / Spectrum Mitigation (IS)

Issues can have both human and technical perspectives, for example:

- Human perspective: A Law Enforcement Agency will tell the MAS vendor that an inmate was able to make calls on a contraband cell phone, thus triggering the MAS vendor to look for additional signals or issues with their existing deployment.
- Technical perspective: RF frequencies and power levels emitted from local cellular towers can be scanned and identified with a basic, inexpensive spectrum analyzer or commercially available cellular analysis tools.

The table below notes potential issues in the three categories discussed above that correctional officials should take into consideration:

Category	Potential Issues
RF, M	MAS coverage not adapting sufficiently quickly to macro network changes
RF, M, IS	MAS coverage leaking out of facility into adjoining neighborhoods
RF, M	Contraband cell phones defeating or bypassing the MAS
RF, M	Correctional officials or individuals on “allow list” not being able to communicate
M	Contraband phones being used to support communications via WiFi

Each issue denoted above has various interpretations and perspectives depending on the individual or entity responsible for it. Below are several perspectives with respect to MAS that were evaluated prior to issuing recommendations.

MAS Vendor Considerations:

- Responsible for keeping the system up and running; repeated unscheduled maintenance
- MAS vendor must act on information from Law Enforcement Agency (i.e., its customer) or changes to RF emanations, which are proprietary to cellular providers

Cellular Provider Considerations:

- Responsible for ensuring high QoS on the network for its legitimate customers
- Impractical to send data on each network change to the MAS vendor
 - Some changes are not permanent or do not affect coverage or power levels; not necessary to inform MAS vendor of these
- Network information in the wrong hands could result in risks to the public network
- MAS contains frequencies and power levels for every local provider; risk to proprietary information

Law Enforcement Agency Considerations:

- Responsible for enforcing federal / state / local laws and regulations; ensuring unauthorized communications are blocked
- Significant financial investment rendered worthless when a communications path opens
- Personnel could be placed at risk due to open communications channel

5.1.1 MAS Best Practice Recommendations

VT-ARC has developed the following recommendations to address the issues highlighted above. These recommendations address the most general issues that occur utilizing a MAS deployment at a correctional facility. Due to the varied designs of correctional facilities throughout the country, each MAS will have its own unique challenges; however, the above issues may occur with any deployment.

- Continual RF planning, testing, and monitoring to ensure control of relative power at correct levels inside and outside the correctional facility.
 - Communication between correctional facility officials, MAS vendors and cellular providers regarding network re-provisioning, inmate activity, and system performance.
- Coordination with general public to address inadvertent RF leakage into the community, prevent spectral interference, and address emergency events (e.g., natural disasters, security incidents)
- Effective control of contraband influx into facilities
- Allow lists to permit authorized communications throughout the facility
- Emergency call and dialed number handling

5.1.2 MAS Deployment Critical Issues and Related Recommendations

The top critical human and technical issues and recommendations to address them are shown below.

Critical Issue 1: MAS coverage needs to adapt quickly to macro network changes

Communications between MAS vendors and macro network providers vary; when they do not communicate and networks are re-provisioned, the MAS may lose the ability to prevent communications.

Recommendation:

- Ensure MAS vendors monitor and react to cellular macro network changes; consider creating lines of communication between cellular providers, correctional facility officials, and CIS vendors to communicate impactful macro network changes while ensuring practices/guidelines are in place to protect cellular provider proprietary information.

Critical Issue 2: 2G Services ending -- Impact on current MAS designs

A typical means for MAS networks to deny service is to step down the User Equipment (UE), e.g., cell phones and hotspots, from 3G / 4G to 2G services to avoid controlled/encrypted authentication at the higher service levels. Cellular providers are already starting to disable 2G services. At some point in the future, UEs may not include 2G functionality, rendering legacy MAS networks ineffective.

Recommendation:

- Create roaming agreements between cellular providers and MAS vendors to enable newer generation services on MAS networks; upgrade MAS designs to “capture” contraband devices without forcing UEs to 2G.

Critical Issue 3: Correctional officials or individuals on “allow list” cannot always communicate

Corrections officials have issues with communicating with each other in certain areas of the facility, particularly in areas where the MAS network would typically handover to the macro network and in locations within the facility with weaker coverage or in between MAS coverage zones.

Recommendation:

- Pursue a “MAS Evolved” roadmap to transition MAS systems from a single-cell uncoordinated system to one that co-exists with the public macro network to permit authorized hand-offs and communications coordination.

Critical Issue 4: Contraband cell phones are enabling unauthorized inmate communications via WiFi

While the two MAS solutions tested succeeded in blocking communications from contraband devices over simulated and actual cellular networks, a CIS system can only do so much to prevent unauthorized communications from occurring. The MAS that were tested were not required to handle WiFi communications as part of their contracts with the correctional institutions. Contraband WiFi hotspots enable prohibited internal communications within a correctional facility. The contraband hotspots can also create a bridge between areas with high CIS coverage to those with little or no coverage and provide an escape path for unauthorized communications.

Recommendation:

- Consider enhancing MAS to block WiFi communication and including requirements for WiFi features in MAS procurements [Note: Recommendation may face legal constraints that bar a MAS solution from blocking WiFi operations on unlicensed spectrum.]

5.2 DSS (JAMMING) SOLUTIONS GUIDELINES AND BEST PRACTICES

Denial of Service Systems (DSS) may be effective at disrupting communications; however, significant hurdles exist in the United States for their use and widespread proliferation. The most notable of these hurdles is the potential for causing harmful interference to valid users outside of a correctional facility, or in adjacent bands. For that reason, 47 U.S. Code § 333 and FCC policy expressly prohibit non-federal operation of jammers in the United States.

If jamming were to be deployed, technical best practices that address the results seen in the lab would include:

- Careful RF design, planning, and maintenance that ensures emanations from DSS do not travel beyond the boundaries of facility
 - Suppression of harmonics to prevent interference with other frequency bands
- Create RF “safe lanes” or terrestrial alternatives for corrections officials’ communications / emergency communications
 - 911 calls
 - Emergency alerts (e.g., severe weather, security)
 - External calls to / from corrections officials
 - Internal calls to / from corrections officials

Lab testing of a particular jamming solution suggested that there are significant technical issues associated with deploying a jammer in a correctional facility. Pending additional testing and analysis to prove that another particular system might be deployed in such a way to avoid harmful interference to other systems (both inside and outside a particular prison environment) avoiding jamming would be considered the only best practice for that technology. Some criteria that should be included in such testing and analysis are included in the Recommendations for Next Steps.

6 RECOMMENDATIONS FOR NEXT STEPS

6.1 MAS EVOLVED

Several of the critical issues highlighted above might be addressed through the evolution of the current/tested MAS technology:

- A typical means for MAS networks to deny service is to step down the User Equipment (UE), e.g., cell phones and hotspots, from 3G / 4G to 2G services to avoid controlled/encrypted authentication at the higher service levels. Cellular providers are already starting to disable 2G services. At some point in the future, UEs may not include 2G functionality, rendering legacy MAS networks ineffective.
- Corrections officials have issues with communicating with each other in certain areas of the facility, particularly in areas where the MAS network would typically handover to the macro network and in locations within the facility with weaker coverage or in between MAS coverage zones.

The solutions to these critical issues enable a path to a potentially lower cost MAS solution by removing RF coverage complexity within the correctional facility and taking advantage of carrier roaming agreements. The “MAS Evolved” concept trades RF coverage complexity within the correctional facility for one that takes advantage of carrier roaming agreements.

This MAS Evolved concept requires a partnership between MAS vendors and carriers via roaming interconnect. In addition to potentially being less costly (for a new installation), it has the potential to increase the MAS feature set to provide better service to correctional facilities. Moreover, a lower cost solution based on small cells could potentially provide effective multilateration by the MAS to identify the location of UEs in and near the correctional facility. MAS vendors and wireless carriers could explore a MAS Evolved solution by taking the following steps:

Phase 1: Roaming Interconnect

- Implement a limited standard Diameter proxy for MAS deployments that allows for authentication of handsets
- Define Roaming use-case and best practices

Phase 2: Smallcell Testing

- MAS providers and prison officials should consider testing multilateration precision across a range of scenarios, in collaboration with roaming authentication from carriers
- Conduct field testing in correctional facility environment of small-cell / location services (LCS) approach leveraging roaming interfaces

6.2 FUTURE TESTING OF DIFFERENT JAMMING SOLUTIONS –FIELD AND LAB

Laboratory testing of one manufacturer’s jammer indicated a strong risk of generating substantial aggregate interference, both in the designed cellular bands, and out of band. This risk multiplies when

multiple jammer units are used in a correctional facility deployment. Harmful interference to multiple communications domains (e.g., commercial cellular services, terrestrial communications including public safety, satellite communications, aviation, etc.) outside a correctional facility could occur. Although the jamming solution that was tested in the CIS Testbed was not necessarily representative of all possible jammers that may be considered for use in U.S. correctional facilities, this risk has not been thoroughly examined. For example, in January 2018, the National Telecommunications and Information Administration (NTIA) in coordination with the Federal BOP tested a jammer designed to prevent cellular communication within a single correctional facility cell.⁵ NTIA’s report noted that:

“Analysis of the jammer’s potential for harmful interference to licensed radio services, if any, outside the targeted prison cell is beyond the scope of [the NTIA] report.”

Testing additional jamming solutions in both laboratory and field conditions would be needed to more fully assess the likelihood about harmful interference.

If any additional tests of jamming solutions were to take place, they should include the following:

- Explicit measurement of aggregate interference from multiple jammers configured to provide useful CIS service to a correctional facility or portion of a correctional facility.
 - What are the interference signal levels inside and outside of the facility?
 - Do the levels outside the facility constitute harmful interference to cell phones operating in public spaces, or to other services operating in adjacent bands?
- Coordination with cellular service providers before, during and after the test to use carrier Key Performance Indicator (KPI) data⁶ to assess the impact of aggregate interference from the jammers at various cell sites in the vicinity.
- Evaluation of the efficacy of jamming as a CIS solution:
 - Do jammers prevent cell phone operations (i.e., connecting to commercial wireless carrier outdoor cells) at appropriate locations inside the facility?
 - What is the range of efficacy: How far from the jammer(s) are cell phones prevented from operating?

Furthermore, to the extent that additional field tests occur, it is recommended that the jammers being used in the field tests be provided to an independent test laboratory to document the operation and performance in a controlled environment, using measurements such as those detailed in this report.

⁵ Reference: NTIA Report TR-18-533, Emission Measurements of a Contraband Wireless Device Jammer at a Federal Correctional facility, June 2018, available at <https://www.its.bldrdoc.gov/publications/download/TR-18-533.pdf>. We note that in early April 2019, BoP conducted an additional jamming test during which NTIA engineers performed measurements of radio emissions to observe and document their characteristics. Reference: U.S. Department of Justice, Bureau of Prisons Tests Micro-Jamming Technology in South Carolina Prison to Prevent Contraband Cell Phones, Press Release (Apr. 12, 2019), <https://www.justice.gov/opa/pr/bureau-prisons-tests-micro-jamming-technology-south-carolina-prison-prevent-contraband-cell>.

⁶ KPI data includes noise measurements (e.g., interference over thermal, receive total wideband power) and performance data (e.g., throughput, connected users).

APPENDIX A: US FREQUENCY BANDS & CIS TESTBED SUPPORT

The following are cellular bands currently in use within the United States, totaling over 1.1 GHz of spectrum. While there are relatively few 2G/3G bands, there are a wide range of LTE bands in use. The table also indicates which bands are supported by the testbed. Two checkmarks indicates support within one of the fully-integrated base stations, whereas one checkmark indicates support within the frequency-reconfigurable base station (S60Z). An “X” indicates that the band is not supported by any of the base stations and was not be included in the testing.

Band Name	Uplink Band (MHz)	Downlink Band (MHz)	Testbed Support
2G/3G Bands			
ESMR	806 – 825	851 – 896	✓ ✓
CLR	824 – 849	869 – 894	✓ ✓
PCS	1850 – 1910	1930 – 1990	✓ ✓
AWS	1710 – 1755	2110 – 2155	✓
LTE Bands			
Band 2	1850 – 1910	1930 – 1990	✓ ✓
Band 4	1710 – 1755	2110 – 2155	✓
Band 5	824 – 849	869 – 894	✓ ✓
Band 12	699 – 716	729 – 746	✓
Band 13	777 – 787	746 – 756	✓
Band 17	704 – 716	734 – 746	✓
Band 25	1850 – 1915	1930 – 1995	✓
Band 26	814 – 849	859 – 894	✓
Band 29	N/A	717 – 728	✓
Band 30	2305 – 2315	2350 – 2360	✓
Band 41	2496 – 2690 TDD		✓
Band 48	3550 – 3700 TDD		✓
Band 66	1710 – 1780	2110 – 2200	✓
Band 71	663 – 698	617 – 652	X
Band 252	5150 – 5250 TDD		X
Band 255	5725 – 5850 TDD		X

APPENDIX B: TABLE OF ACRONYMS

Abbreviation	Meaning
2G	Second Generation Cellular Technology
3G	Third Generation Cellular Technology
4G	Fourth Generation Cellular Technology
AC	Alternating Current
ASCA	Association of State and Correctional Administrators
BOP	Federal Bureau of Prisons
BRS	Broadcast Radio Service
BTS	Base Transceiver Station
CBRS	Citizens Broadband Radio Service
CDCR	California Department of Corrections and Rehabilitation
CDMA	Code Division Multiple Access
CDS	Cell Detection System
CDS-A	Active Cell Detection System
CDS-P	Passive Cell Detection System
CID	Cell ID
CIS	Contraband Interdiction System
CLR	Cellular
DAS	Distributed Antenna System
DC	Direct Current
DL	Downlink
DOC	Department of Corrections
DOJ	Department of Justice
DSS	Denial of Service System
DUT	Device Under Testing
EARFCN	E-UTRA Absolute Radio Frequency Channel Number
EBS	Education Broadband Service
EDGE	Enhanced Data GSM Environment
EIRP	Equivalent Isotropic Radiated Power
eNB	Evolved Node B
E-UTRA	Evolved Terrestrial Radio Access
EV-DO	Evolution Data Optimized
FCC	Federal Communications Commission
FDD	Frequency Division Duplex
GPS	Global Positioning System
GSM	Global System for Mobile communications
GSMA	GSM Association
GTL	Global Tel Link
GUI	Graphical User Interface

IDAS	Indoor Distributed Antenna System
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
KPI	Key Performance Indicator
LCS	Location Services
LNA	Low Noise Amplifier
LTE	Long Term Evolution
MAS	Managed Access System
NB	Node B
NOC	Network Operations Center
NTIA	National Telecommunications and Information Administration
oDAS	Outdoor Distributed Antenna System
OS	Operating System
OSS	Operations Support System
PCI	Physical Cell Identifier
PCS	Personal Communications Service
PN	Pseudo Noise
PSAP	Public Safety Answering Point
RAN	Radio Access Network
RAT	Radio Access Technology
RF	Radio Frequency
RHU	Restricted Housing Unit
RSRP	Reference Signal Received Power
RSSI	Received Signal Strength Indicator
SCDC	South Carolina Department of Corrections
SDR	Software Defined Radio
SIM	Subscriber Identity Module
SMA	SubMiniature version A (connector)
SMJ	Shielded Micro Jammer
SMS	Short Message Service
SOP	Standing Operating Procedure
SOW	Statement of Work
SSID	Service Set Identifier
TDCJ	Texas Department of Criminal Justice
TDD	Time Division Duplex
UE	User Equipment
UL	Uplink
UMTS	Universal Mobile Telecommunications System
UPS	Universal Power Supply
USIM	User Services Identity Module
VoLTE	Voice Over LTE
VPN	Virtual Private Network

VSG Vector Signal Generator
VT-ARC Virginia Tech Applied Research Corporation