

The Efficacy of Managed Access Systems to Intercept Calls from Contraband Cell Phones in California Prisons



California Council on Science and Technology
May 2012

The Efficacy of Managed Access Systems to Intercept Calls from Contraband Cell Phones in California Prisons

May 2012

California Council on Science and Technology

ACKNOWLEDGEMENTS

We would like to thank the many people who provided input towards the completion of this report. Without the insightful feedback that these individuals generously provided, this report could not have been completed. We would like to give special thanks to Charles Harper, CCST Board Member and chair of the project team that developed this report, and S. Pete Worden, director of the NASA Ames Research Center, who provided technical experts who contributed to and reviewed this report.

This report was conducted with the oversight of a CCST Contraband Cell Phones in Prisons Project Team, whose members include: Charles Harper, chair of the CCST Project Team, Patrick Diamond, Brian W. Carver, with technical expert input from NASA Ames Research Center via S. Pete Worden, director, NASA Ames Research Center, Don Beddell, Robert Cates, Deb Feng, Ray Gilstrap, William Hunt, and William Notley, James Williams, and the Charles Stark Draper Laboratory via David Goldstein, senior systems engineer. We also thank Lora Lee Martin, CCST Director Sacramento Office, for the overall project coordination resulting in this report. We express gratitude to CCST's members and colleagues for their many contributions to the report and substantive peer reviews that were conducted. A more complete list of the project team is included in Appendix 1.

This document was prepared under a grant from FEMA's Grant Programs Directorate, U.S. Department of Homeland Security. Points of view or opinions expressed in this document are those of the authors and do not necessarily represent the official position or policies of FEMA's Grant Programs Directorate or the U.S. Department of Homeland Security.

COPYRIGHT

Copyright 2012 by the California Council on Science and Technology. Library of Congress
Cataloging Number in Publications Data Main Entry Under Title:
The Efficacy of Managed Access Systems to Intercept Calls
from Contraband Cell Phones in California Prisons
May 2012
ISBN 13: 978-1-930117-63-1

The California Council on Science and Technology (CCST) is an independent non-profit 501(c)3 organization established in 1988 at the request of the California State Government. CCST's mission is to improve science and technology policy and application in California by proposing programs, conducting analyses, and recommending public policies and initiatives that will maintain California's technological leadership and a vigorous economy.

Note: The California Council on Science and Technology has made every reasonable effort to assure the accuracy of the information in this publication. However, the contents of this publication are subject to changes, omissions, and errors, and CCST does not accept responsibility for any inaccuracies that may occur.

For questions or comments on this publication contact:

California Council on Science and Technology
1130 K. Street, Suite 280
Sacramento, California 95814
(916) 492-0996
ccst@ccst.us

Table of Contents

Transmittal Letter from CCST	1
Letter of Request from the California Legislature	3
1. Key Report Findings	6
2. Recommendations	7
3. Legislative Request	8
4. Project Approach	8
5. Statement of Problem	9
6. Legal and Regulatory Context	10
7. Overview of Contraband Cell Phone and Wireless Technology	12
8. Stopping Illicit Cell Phone Use in Prisons	13
9. What is Happening Nationally and in Other States	15
10. Review of Managed Access System (MAS) Technology	15
11. Limitations of Managed Access System Technology	20
12. Can California Develop a Successful MAS Model?	21
13. Benefits of a Robust Pilot Project	23
14. Third Party Consortium Oversight	24
Appendix 1: CCST Project Team Members	26
Appendix 2: CCST Letter to Senators Identifying IFB Issues of Concern (October 29, 2011)	27
Appendix 3: Letter from Senators to Matthew Cate, Secretary, California Department of Corrections and Rehabilitation (CDCR) Conveying Issues from CCST's October 2011 Letter	29
Appendix 4: Preliminary List of Issues Identified with Status Updates.....	34
Appendix 5: April 11, 2012 Letter from Senators to Secretary Cates, California Department of Corrections and Rehabilitation (CDCR) Conveying Notice of the Immanence of the CCST report	36
Appendix 6: An Analysis of Barriers to Implementing Airport-Style Security at all Points of Entry to California's Correctional Institutions, January 2012.....	38
Appendix 7: Federal Bureau of Prisons Electronic Search Protocol	45
Appendix 8: What is Radio Frequency (RF) Communications - The Idea of Waves as Energy.....	47
Appendix 9: Technical Evaluation Report: CCST Challenges, Sandia National Laboratory, April 2012	63
Bibliography - Source Documents	68
Glossary.....	70

Transmittal Letter from CCST Regarding Report



CALIFORNIA COUNCIL ON SCIENCE AND TECHNOLOGY

Sustaining Members

*University of California • California State University
California Community Colleges • California Institute of Technology
Stanford University • University of Southern California*

Laboratory Affiliate Members

*Lawrence Berkeley National Laboratory
Lawrence Livermore National Laboratory • Sandia National Laboratory
Stanford Linear Accelerator Center • NASA Ames • Jet Propulsion Laboratory*

May 2, 2012

Senator Elaine Alquist
Senator Loni Hancock
Senator Christine Kehoe
Senator Alex Padilla

Subject: Contraband cell phones in California prisons

Dear Senators,

We thank you for the request to do this study regarding technological approaches for preventing the use of contraband cell phones in prisons. The foresight of the Senators to request a review of the investment that this report covers and the effectiveness of that investment is commendable. California again has the opportunity to be on the cutting edge of technological investment, this time in public safety. However, as you will also see in this report, achieving this leadership position in the development and deployment of the technology should be done with a full understanding of its abilities and limitations.

CCST was asked by members of the California State Senate to analyze the overall issue of contraband cell phones as well as the viability of a specific proposed system for managing cell phone access in prisons, Managed Access Systems (MAS). As many have noted, the issue of contraband cell phones is complex and will require a multipronged approach to address. Procedures being pioneered in the federal prison system to limit the influx of contraband devices offer valuable strategies for California to consider, including the use of metal detectors and entry searches for all staff and visitors – a standard practice in federal facilities, but one which is not followed in all state prisons. The federal government is also working in partnership with the cell phone industry to disable stolen cell phones, making them useless; it is likely many of those stolen phones have found their way into the prisons or that the approach can be extended to locate and disable phones not approved for use in a specific prison.

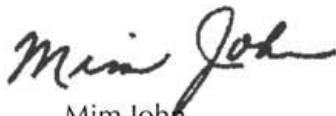
As for the proposed MAS recently contracted for by the California Department of Corrections and Rehabilitation (CDCR) for managing cell phone access in prisons, our conclusions are clear: the technology shows promise, but it is not ready for deployment. In point of fact, there are no prisons anywhere in the United States using a fully functional managed access system to control cell phone use. The preliminary testing conducted so far in California has been extremely limited in scope and scale, essentially a proof of concept trial rather than a full-fledged pilot program that takes into account the complexities of interference from the prison structure itself and surrounding locale. Furthermore, MAS is not the only technology that could

full investment in MAS. California could again be on the cutting edge of developing new technologies but do to do so, as noted in this report, requires the development of robust pilot project deployments of MAS or other technologies being considered.

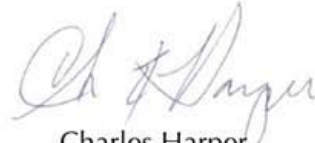
We note that as this report was being reviewed for technical accuracy and finalized for release, the California Department of Corrections proceeded to contract for a MAS. We appreciate that the management of the state's prisons is a large and complex issue, and that action is needed on this pressing issue. However, a long-term statewide investment in this technology before it is proven is, in our opinion, unwise. Our recommendations are in line with the report provided by the Inspector General in 2009, which supported steps such as investing in more thorough screening of all personnel entering and leaving the confined prison environment.

Our mandate is to provide the best possible impartial science and technology expertise and advice to California state policymakers. The role of safeguarding our state's prison system is a difficult and often thankless task. It is precisely for this reason that we believe California must plan carefully how best to manage the issue of contraband cell phones in prisons, and invest in research and development that will produce a system which meets the needs of the state through deployment of mature and tested technology.

Sincerely,



Mim John
CCST Council Chair



Charles Harper
CCST Board Member and CCST Project Team Chair



Karl Pister
CCST Board Chair



Susan Hackwood
CCST Executive Director

Letter of Request from the California Legislature

CALIFORNIA LEGISLATURE

STATE CAPITOL
SACRAMENTO, CALIFORNIA
95814

July 7, 2011

Mr. Karl Pister, Chair
Ms. Susan Hackwood, Executive Director
California Council on Science and Technology
1130 K Street, Suite 280
Sacramento, CA 95814-3965

Dear Mr. Pister and Ms. Hackwood,

We are writing to request a study by the California Council on Science and Technology (CCST) regarding the technology to prevent the use of contraband cell phones in California prisons.

The smuggling and use of contraband cell phones is a troubling international public safety concern that in recent years has expanded dramatically in California. At the 33 institutions of the California Department of Corrections and Rehabilitation (CDCR), 261 cell phones were confiscated in 2006, rising to more than 10,000 in 2010. The bottom-line question is, what is the best way to prevent cell phones from getting into the hands of inmates, and if they do, how best to prevent calls from being completed without impairing the ability of prison authorities to make and receive official business cell phone calls?

Recently, CDCR announced that they conducted a pilot study of "managed access" technology to capture and prevent the completion of contraband cell phone signals. The trial was run at two undisclosed prisons for 96 hours, though at one facility it was conducted in a limited location and for a much shorter time period due to system overload and crash. This technology was previously tested and/or employed in Mississippi, Maryland, and South Carolina prisons and was featured in a December 2010 report released by the National Telecommunications and Information Administration and U.S. Department of Commerce, *Contraband Cell Phones in Prisons, Possible Wireless Technology Solutions*.

CDCR is proceeding to go to bid and award a six-year contract early next year for all 33 of its prisons. The contracted vendor would also provide landline telephone services, which presumably would greatly increase due to the immobilizing of standard mobile phones. However, an independent, scientific evaluation by the CCST will help inform both policy makers and the public about the technology being considered by the CDCR to determine if this approach is the most effective, feasible, and economical for California. To that end, we request that the CCST research the following:

- 1) **Describe the Availability and Feasibility of Managed Access Technology:**
 - a) A technical description with advantages and disadvantages of its use, including whether the CDCR pilot program lasted long enough to be valid.

- b) A cost-benefit analysis including the costs of installation, staff training, management, and ongoing operation.
 - c) The feasibility of implementing managed access technology in California prisons given the numerous facility variations in size, structural complexity, and geography/topology.
 - d) A review of the characteristics and results of its use in other states or nations.
- 2) Alternatives to Managed Access:**
- a) What are the alternative technologies currently available?
 - b) What are the promising, cutting-edge technologies not yet on the market?
 - c) Review the efficacy of providing inmates with email communication to family and friends as a solution, compared to managed access (in terms of security, cost, etc.).
- 3) Potential Hacking, Overriding, and/or Circumventing of Managed Access and Other Systems:**
- a) What are the available technologies or techniques used to override, hack, or otherwise circumvent managed access technology or other signal-blocking/detection technologies?
 - b) What upcoming technologies could be used for those purposes?
 - c) How long would it take to hack or override the managed access system or other technologies? How difficult would it be?
- 4) Limitations of Signal Capture and Control:**
- a) Can the managed access system or the other available technologies capture all cell phone frequencies and wireless communications currently on the market? Is it technically possible to anticipate future technologies? How feasible is it for the managed access system to be continually upgraded for emerging technologies, and at what cost?
 - b) Will all calls, texts, e-mails, and Internet activity be blocked? What about cell phones whose frequencies can be switched automatically or manually when one mode of connection is not available?
 - c) What about Skype and satellite phones which can bypass commercial network base stations entirely?
- 5) Societal Impacts:**
- a) What are the societal impacts of the available technology? How will the general public living near or commuting around prisons be affected, if at all? What is the possibility of their calls being intercepted?
 - b) What are the privacy, wire-tapping/pen-register, or other legal concerns regarding these technologies?
- 6) Other Examples and Options:**
- a) Please provide a review of the Federal prison system's response to contraband cell phones, particularly the federal prisons in California. What is the feasibility and estimated cost of implementing a comparable system in California state prisons?
 - b) What types of metal detectors or other screening technologies, including but not limited to infrared devices, could CDCR employ to prevent mobile calling devices

- from being introduced into prisons? Are CDCR's existing metal detectors up for the task? What would be the cost of additional metal detectors?
- c) What is the most effective way to deal with contraband cell phones? What is the most sophisticated, state-of-the-art response? Include international examples.

We propose both an open-ended deadline of sometime late this fall or early winter that will provide the CCST the time to complete a comprehensive report, while also requesting a preliminary report within 3-4 months. The content of this preliminary report would be contingent upon the topics the CCST could cover within that timeframe. We leave that to the CCST's discretion.

Thank you for your consideration of this request on this important issue.

Sincerely,



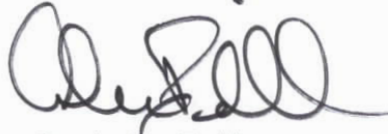
Senator Elaine Alquist



Senator Loni Hancock



Senator Christine Kehoe



Senator Alex Padilla

1. Key Report Findings

Contraband Cell Phones in Prisons are a Growing State and National Security Issue

In 2011, approximately 15,000 contraband cell phones were confiscated at the California State Prisons.¹ This represents only the cell phones found, not all phones in the facilities. Though the phones may be used for communications with family or for entertainment, they can also be used for illegal or dangerous activities. This California Council on Science and Technology (CCST) report acknowledges that a suite of technological and non-technological approaches to address this problem is warranted.

Inconsistent Screening at State Prisons

Screening of California Department of Corrections and Rehabilitation (CDCR) personnel and visitors entering and leaving the prisons was found to be less rigorous than screening found at a normal airport security screening access point. During visits to several prison facilities, unscreened items, e.g., purses, duffle bags, and large soft-sided ice chests, were seen both entering and leaving CDCR facilities without x-ray, metal detection, or thorough manual searches.

Existing and Evolving Complexities of Signal Capture

There are significant technological challenges to effective implementation of MAS and other approaches based on the evolving capabilities of mobile devices. This includes capabilities seen in mobile devices in the marketplace today and the anticipated future capabilities of commercial mobile devices including satellite phones.² This complexity argues for an investment in securing the contraband devices themselves rather than reliance on technology to block the communication.

MAS Technology Not Yet Proven for Prison Environment

CCST finds that the Managed Access System (MAS) technology of today is not mature enough for immediate large-scale deployments such as that proposed by CDCR at California's 33 state prisons.

MAS Efficacy Protocols Not Defined

CCST notes that there is no evidence that CDCR has fully or reliably identified the size of the contraband cell phone problem or a mechanism to determine the efficacy of a MAS when deployed.

Baseline Benchmarks Needed

To evaluate the effectiveness of an installed MAS, a baseline measure of contraband cell phone usage must be done prior to implementing a MAS strategy.

¹ CDCR personnel provided these numbers orally to the CCST project team at a CDCR briefing on January 5, 2012 held at the California Senate Office of Research and again at a prison tour on January 10th, 2012.

² Technical Evaluation Report: CCST Challenges, Sandia National Laboratories, April 19, 2012 (See Appendix 9)

2. Recommendations

Alternative options for mitigating Contraband Cell Phones should be considered before adoption of MAS or use of other technologies

MAS, even if successfully designed and deployed, is not enough. Other options (technical and non technical) for managing the cell phone problem should be aggressively pursued. Undertake a comparative benefit/cost for these other options that include:

1. **Implement the Federal Prisons Screening Protocols in California Prisons- Airport like security screening** at all entrances for all personnel and all items.
2. **Conduct thorough searches of all items, vehicles, and personnel at all sally port entrances** using all available means to identify contraband.
3. **Test the use of other technologies within confined prison locations**, (e.g., prison cell block or technologies to identify and locate transmissions) to intercept and dead-end unauthorized cell phone calls.
4. **Engage the cell phone carriers to identify use of their technology and to deny connections** for unregistered cell phones from within prison locations.
5. **Pursue, in coordination with other states and federal legislators, prison specific exceptions to Federal Communications Commission (FCC) anti jamming regulations.** This approach would be complementary to the federal government's 2012 agreement with vendors to disable stolen cell phones.

However, if MAS is pursued then pursue it wisely: Independently test one or more pilots before contracting for a MAS.

An independent consortium should be created to develop and oversee the design and deployment of a MAS Pilot Network. The consortium should include technical expertise from research organizations, cellular network operators, and from the California Legislature, (e.g., the Senate Office of Research). The consortium should be overseen and managed by an independent third party with technical credentials suited to the task.

Design, Install and Monitor MAS Pilot(s).

One or more pilot projects should be installed and operated for at least 12 months **prior to contracting for deployment of a CDCR MAS** to provide;

1. Identifiable measures of efficacy for the MAS regarding the volume of cell phone usage before and volume of blocked calls after the MAS deployment.
2. A working template for implementing the MAS in the demanding environment of a correctional institution.
3. The operational expertise of cell phone network operation within the CDCR and/or California Technology Agency (CTA).
4. A mechanism for third party oversight of the MAS operation and conformance to wireless operations standards including a mechanism to measure vendor compliance to emerging wireless technology and deployment modernization techniques.

3. Legislative Request

This report is in response to a July 7, 2011 letter of request to the California Council on Science and Technology (CCST) from four California State Senators (Senators Elaine Alquist, Loni Hancock, Christine Kehoe and Alex Padilla). As detailed in the front of this report, the senators asked CCST to provide input on the best way to prevent cell phones from getting into the hands of inmates and, if they do, how best to prevent calls from being completed without impairing the ability of prison authorities to make and receive official business cell phone calls. In addition, they asked CCST to undertake a study on the feasibility of Managed Access Systems (MAS) technology as an effective strategy to curtail the use of contraband cell phones in the California State Prisons. In their letter the senators indicated that the California Department of Corrections and Rehabilitation (CDCR) had issued an Invitation for Bid (IFB),³ for replacement of the Inmate and Wards Telephone System (IWTS) including a requirement and specifications for the installation and operation of a MAS at each of the 33 State Prison sites to combat the problem of contraband cell phones in the California State Prison system. In exchange for the MAS system, the successful bidder/vendor would receive the right to operate and collect revenues from the IWTS landline phone system. Across all of the California prison facilities this IWTS use is estimated to be approximately 99 million minutes of landline calls. The CDCR IFB defines in detail the required parameters for the IWTS and the MAS.

4. Project Approach

CCST convened a Contraband Cell Phone Project Team comprised of CCST council and board members supplemented with additional experts (see Appendix 1 for Project Team Members). The CCST Project Team reviewed in detail the CDCR IFB calling for MAS. From that review, the team identified 12 issues of concern that they conveyed by letter to the State Senators requesting the report (see Appendix 2, CCST Letter to Senators, October 28, 2011). The Senators then transmitted a letter expressing concern to the CDCR (see Appendix 3). Some, but not all, of these issues were subsequently addressed in IFB modifications or clarifications. Appendix 4 contains a summary and status table of these issues. A second letter was transmitted to CDCR on April 11, 2012 by the Senators conveying the immanence of the CCST report and suggesting that the information contained in the document would assist CDCR (see Appendix 5). However, CDCR moved ahead with a contract for MAS on April 16, 2012.

The project Team identified and reviewed many publications and postings about MAS and contraband cell phones in prisons and contacted numerous experts, users, and vendors to understand their current capabilities and limitations. CCST Project Team members met with representatives from CDCR and the California Technology Agency (CTA) for a contraband cell phone interdiction briefing on January 5, 2012, lead by CDCR Cell Phone Interdiction Manager, Tim Vice.

It is important to note that CCST has not undertaken primary research of its own to address these issues. This response is limited to soliciting input from technical experts and to reviewing and evaluating available information from past and current materials related to MAS and contraband cell phones. This report has been approved by the CCST Project Team and has been subject to the CCST's substantive peer review process.

In January 2012, members of CCST's technical team visited two California prisons (Solano State Prison and the California Medical Facility); a separate visit to Folsom State Prison in March also

³ Invitation for Bid (IFB) was issued by the California Technology Agency on behalf of CDCR on July 7, 2011; IFB 11-126805

provided some insights. In discussions with inmates, the CCST team was told that contraband cell phones are paid for in cash, outside the prison, before the phones are smuggled into the prison and delivery is made. It is unclear how many cell phones are being smuggled in; however, the fact that 15,000 cell phones were confiscated last year, as reported to the project team by CDCR personnel⁴, means that many more are likely making their way into the prisons undetected. CDCR indicated that its ability to detect this illegal activity is limited due to the large and varied communities of people entering and leaving the prisons and the many access points into the confinement area. Once contraband phones are inside the prison confinement areas, CDCR has also indicated that their ability to detect cell phone presence is limited. Inmates have numerous ways to hide them, and the CCST team was told that the cell phones are generally used after “lights out” in the confinement areas. The CDCR is exploring the MAS as a potential way to neutralize the smuggled phones, by making them essentially inoperable within the prison confinement area.

Though the CCST Project Team reviewed the entire referenced IFB, it focused specifically on the MAS portion of the IFB. This report details the technical and operational issues of the MAS as the principal approach to help mitigate the contraband cell phone problem. However, we note that there are other technological and non-technological methods that should be considered.

The report identifies and provides details about the few known vendors of these systems. It also identifies performance issues relating to the efficacy of the MAS in mitigating contraband cell phone operation and use.

For context, this report also summarizes the approach taken by the Federal Bureau of Prisons (FBOP) to manage contraband cell phone issues at the point of entry into their facilities. The Federal Bureau of Prisons has been instructed by the U.S. Government Accountability Office (GAO) to coordinate with states to identify a uniform approach to addressing this problem.⁵

This report mainly addresses the issue of contraband cell phones using their native cellular capabilities, including voice, text message and data services. Though mentioned in this report, the operation of contraband cell phones using secondary communication capabilities such as point-to-point wireless LAN (e.g. Wi-Fi) or short-range RF (e.g. Bluetooth) communications is not explored in great depth.

5. Statement of Problem

Contraband cell phones are being smuggled into California State Prisons in large numbers. According to the prisoners that the project team interviewed, the cell phones are used, in large part, for communications with inmate family members and friends or for entertainment (e.g., gaming or videos). However, the use of these contraband cell phones also has numerous negative effects as reported by recent reports from the Federal Bureau of Prisons,⁶ U.S. Department of Commerce,⁷ and several independent state corrections departments.⁸ These negative effects include illegal activities such as drug deals, gang operations, victim harassment and instructions for ‘hits’.

4 At a CDCR briefing on January 5, 2012 held at the California Senate Office of Research and again at a prison tour on January 10th, 2012, CDCR personnel provided these numbers orally to the CCST project team

5 U.S. GAO 11-893 Bureau of Prisons: Improved Evaluations and Increased Coordination Could Improve Cell Phone Detection, September 2011

6 U.S. GAO Report to Congressional Committees; “Bureau of Prisons – Improved Evaluations and Increased Coordination Could Improve Cell Phone Detection”, September 2011

7 U.S. Department of Commerce “Contraband Cell Phones In Prisons – Possible Wireless Technology Solutions”, December 2010

8 Special Report, Office of the Inspector General, State of California, May 2009, “Inmate Cell Phone Use Endangers Prison Security and Public Safety”

Contraband cell phones in the prisons can result in:

1. Inmates using these contraband cell phones to operate or control criminal activities from inside the confinement of a prison.
2. Growing inmate demand for illegal smuggling of contraband material into the prison.
3. An untraceable method for inmate communications with people inside and outside the confinement area.
4. Inmates using contraband cell phones to circumvent the fee based pay phone systems established to facilitate inmate calls. The CDCR indicates that this circumvention has a negative financial impact to the provider operating the prison pay phone system. In those states where a portion of the revenue from the use of landlines is reinvested in prison rehabilitation programs, there is a financial loss for the rehabilitation programs.

The risk of illegal activities being performed over these cell phones prompts the need for solutions and intervention approaches to be identified and deployed. The value of contraband cell phones smuggled into prisons can be up to \$1000 per smuggled phone⁹ (this cost is in addition to the external costs of phone purchase and service agreements with the carrier).

6. Legal and Regulatory Context

In general, the current legal ramifications of smuggling, concealing and/or possessing cell phones in prisons (state and federal) are minimal. Obviously, they are not enough of a deterrent to stop the movement of or access to these technologies. They are, nonetheless, a start.

Federal Laws and Regulations

In August 2010, the Cell Phone Contraband Act of 2010 was passed and amended 18 U.S.C. § 1791 to prohibit an inmate of a federal prison from possessing, obtaining, or attempting to obtain a cell phone.

California State Laws and Regulations

CA SB26 was passed and enacted in 2011 making possession of a cell phone by an existing prisoner a misdemeanor. This bill would provide, with exceptions, that a person who possesses with the intent to deliver, or delivers, to an inmate or ward in the custody of the department any cellular telephone or other wireless communication device or any component thereof, including, but not limited to, a subscriber identity module or memory storage device, is guilty of a misdemeanor, punishable by imprisonment in the county jail not exceeding 6 months, a fine not to exceed \$5,000 for each device, or both the fine and imprisonment. An inmate found in possession of a wireless communication device will be subject to a time credit denial or loss of up to 90 days. This law also provides “deemed consent” inside the secure perimeter of a correctional facility to utilize technologies such as the Managed Access Systems.

Governor of California Executive Order B-11-11: Contraband Cell Phones

This Executive Order, issued upon passage of SB26 directs CDCR to take additional steps to control the proliferation of contraband cell phones, including preventing them from penetrating beyond the prison’s secure walls and to immediately review and prepare an

⁹ During a tour of the Solano State Prison and the California Medical Facility on January 10th, 2012 CCST Project Team members learned this from discussions with prisoners.

analysis of any barriers to implement airport-style security screening at all points of entry to California's correctional institutions, and that this analysis be submitted to the Governor's Office by December 31, 2011.¹⁰ The order also required, among other things, that the CDCR implement a system to intercept and block prisoners' unauthorized cellular transmissions. The CDCR is currently in a competitive procurement to install a permanent MAS in collaboration with the Federal Communications Commission to meet this mandate consistent with federal law at the majority of its correctional facilities.¹¹ A copy of this report was provided to CCST as we were finalizing this report (Appendix 6). From a review of the report it appears that the cost of implementing full screening at each of the prison facilities as summarized in this report is likely no more expensive than the estimated \$1 million per prison estimated for MAS installation.

[Special Report: Inmate Cell Phone Use Endangers Prison Security and Public Safety – Office of the Inspector General](#), State of California, May 2009 (D. Shaw, Inspector General). The security issues related to contraband cell phones have been understood by the state for some time. The Inspector General (Shaw), in his transmittal letter addressed to Secretary Cate, CDCR, May 4, 2009¹² stated:

"...the Office of the Inspector General found that the possession of cell phones in prison facilities by inmates has increased significantly during the past three years and poses a threat to the safety and security of California's prison staff, inmates, and the general public. We also found that the growing number of cell phones in prison facilities is a direct indicator that the methods used by the California Department of Corrections and Rehabilitation to interdict their introduction or possession have mostly proven ineffective."

To truly eradicate contraband cell phone usage the Office of the Inspector General recommended that the Secretary of CDCR take the following actions. The recommendations are similar to CCST's current recommendations in this report (Appendix 7).

10 CDCR PowerPoint Presentation to CCST Team by T. Vice, Cell Phone Interdiction Manager, CDCR, Jan. 5, 2012..

11 Letter from Secretary Cate, CDCR to Ms. Robinson, Assistant Attorney General, US Department of Justice, October 31, 2011

12 Special Report: Inmate Cell Phone Use Endangers Prison Security and Public Safety – Office of the Inspector General, State of California, May 2009; Page -2

Office of Inspector General Recommendations

1. Continue efforts to seek legislative change to make the introduction or possession of cell phones in all correctional facilities a criminal offense;
2. Collaborate with other state and federal correctional agencies to lobby the Federal Communications Commission (FCC) for an exemption in using cell phone jamming devices;
3. Request additional funds to purchase cell phone detection solutions and jamming devices (if subsequently approved by the FCC);
4. Request resources and funds to conduct airport-style screening including metal and canine detection, and when necessary, manual searches of persons entering California prison facilities;
5. Restrict the size of all carrying cases being brought into the secure areas of prisons by all persons including backpacks, briefcases, purses, ice chests, lunch boxes, file boxes, etc., so that they may be x-rayed;
6. Require staff and visitors to place all personal items in see-through plastic containers;
7. Request additional resources and funds to increase detection activities similar to "Operation Disconnect;"
8. Ensure all quarterly contract vendor packages be shipped directly to prisons and correctional camps; and
9. Implement an anonymous cell phone smuggling reporting system for employees and inmates.

7. Overview of Contraband Cell Phone and Wireless Technology

The following section defines key terms and describes the operation of wireless communication technologies. More detail is provided in Appendix 8. In addition, a technical evaluation was provided by Sandia National Laboratories (Appendix 9). We note that the latter also describes possible other technologies that could be considered in a pilot program.

In this report, the term "cell phone" refers to a radio-telephonic instrument used to make telephone calls, send and receive text (SMS and MMS) messages, or send and receive data using licensed radio spectrum. The term "contraband cell phone" is used to denote those cell phones in the unauthorized possession of inmates within prisons.

Cell phones and devices can be used in many different ways. While the original intent was longer-range wireless communications, current advances in technology have increased the computing power of a cell phone so substantially that new and emerging uses are being discovered every day. These advances in technology have essentially resulted in a computer that can fit in a pocket. Today's cell phones are more capable than computers were just a few years ago. In addition, computer operating systems extend usefulness of the cell phone to a full computing environment. It is expected that this evolution of technology will continue at the same or faster rate resulting in an ever-increasing expansion of the functions of cell phones.

Wireless Communications

Cellular phones are now commonplace for long-range wireless communications, via voice, text message or data. The cell phone has become a ubiquitous assistant that is attached to nearly every one of us during our daily routines. More and more often, the cell phone is becoming the only phone for many people. The estimated penetration rate of cell phone volume versus population in the U.S.,

for example is in excess of 100%,¹³ and is even greater in many other countries¹⁴.

With the increasing capability of the cellular phone serving as a hand held computer, numerous additional communications methods are being integrated into the device at a rapid rate. Included in this expanding suite of capabilities are Wi-Fi and Bluetooth.

- Wi-Fi is the most common wireless local area network (WLAN) technology used for wirelessly connecting computers and devices to one another.
- Bluetooth is a form of a wireless, short-range, personal area network (PAN) that is used to connect devices together in close proximity, such as cell phones and headsets. Bluetooth is a public domain wireless standard under governance of the Bluetooth Special Interest Group (SIG).

These two capabilities alone enable the potential use of cellular phones for short-range communications within the prison, e.g., between prisoner cells or between prison cellblocks.

Unlike the more traditional method of cellular phone communications, which rely on an infrastructure network with towers and carriers, short-range communications can be accomplished without fixed or existing infrastructure for operation. This short-range communications capability could result in the ability for an inmate to call other inmates in close proximity and send data files within range (up to hundreds of yards).

Smart Phones and Pocket Computers

Cell phones with multiple functions (including internet access) are referred to as “smart phones”. Most modern cell phones have an array of embedded sensors and tools that can be used independently of any cellular network. At a minimum, virtually any new smart cell phone now has a keyboard, a camera and a flash memory card, such as microSD. Use of these features allows inmates to provide instructions, in the form of written text and/or imagery that can be stored onto a microSD memory card, the size of a fingernail. The memory card can then be easily moved around a cellblock, or transferred to somebody on the outside, providing a delayed communications channel independent of the cellular network.

8. Stopping Use of Illicit Cell Phone Use in Prisons

Finding Phones at Entry Points

A primary response to the problem of contraband cell phones in prisons should be to more thoroughly inspect all personnel entering and leaving the prisons, the confinement area, and all accessible spaces, as well as the prisoners themselves. Installation and operation of airport-like screening points would help ensure that personnel and visitors were not carrying in or out contraband items including cell phones. Even manual searches would likely capture at least some potential contraband or deter its entry. In some cases cell phone-sniffing dogs have been used to successfully screen incoming vehicles and packages for contraband cell phones.¹⁵ Thorough screening at California State Prisons (similar to screening at federal prisons, addressed later in this report) should be both an expected and reasonable approach for California to implement. However, from the January 2012 CDCR briefing and team member visits to prisons, the CCST Project Team learned that ‘airport’ level screening of CDCR personnel and, in some cases even visitors, is limited or nonexistent. CDCR personnel were observed carrying duffle bags and soft-sided ice chests in and out of the prison without thorough screening.¹⁶ The fact that metal detectors or more rigorous manual searches are not routinely and

13 http://ctia.org/media/industry_info/index.cfm/AID/10323

14 <http://www.parl.gc.ca/content/LOP/ResearchPublications/prb0826-e.htm#penetration>

15 http://www.nj.com/news/index.ssf/2011/12/cell_phone-sniffing_dogs_used.html

16 CCST visit to Folsom State Prison in March 2012 did include metal detector screening of people but all possessions

rigorously implemented as a first line of defense at all California correctional facilities was a surprise and concern to the CCST Project Team.

The CCST Project Team recommends that thorough screening of all personnel, items, and vehicles be implemented consistent with the Federal Bureau of Prisons protocol (Appendix 2) and the 2009 recommendations of the California Inspector General (Appendix 9).

Identifying/Tracking Phone Use

Numerous technical methods exist for identifying a cell phone via the radio signal emitted by the phone. Detection systems to identify this radio frequency signal vary in cost and complexity from simple hand held devices to highly sophisticated systems capable of detecting both the use and the location of the cell phone. These systems still require human engagement to assess detector outputs and inspect the confinement area for the contraband phone. It should be noted that any method requiring prison correctional officers to actively participate would likely arouse the suspicion of the inmates. As a result, it is expected that when correctional officers begin inspecting an area of the prison, prisoners would turn off contraband cell phones, therefore nullifying the efficacy of the detection system. The limitations of this search approach calls for alternatives or companion approaches for eradication of contraband cell phones use. Because of the difficulty in physically finding the cell phones, the idea of automatically rendering contraband cell phones inoperable is attractive to prison control organizations. This promise of an “automated” mitigation system has sparked interest in the MAS installations in prisons; however, the CCST Project Team only found evidence of one such system installed at a single prison in Mississippi and understand that this system is not yet fully operational.

The CCST Project Team recommends that potentially useful technology approaches be explored in confined prison areas, and that cell phone carriers be engaged to explore options of denying connections for ‘unregistered’ cell phones within prison locations using the carriers’ technology. In this latter case, identity of illegal cellular phones could be obtained via a benchmarking technology and the carrier could then deny cellular connection to the specific unregistered devices. Engaging the carriers would likely require either a legal requirement to participate or an income incentive via fee for participation. With the recent agreement of cell phone carriers with the federal government to disable services on stolen cell phones, this approach should be explored¹⁷.

Explore Prison Specific Jamming Approvals

The Federal Communications Act of 1934 prohibits the use of jamming technologies. However, as the concern about contraband cell phones in prisons expands, there is growing interest in seeking exception to this law to allow jamming within the prison environment. South Carolina prison officials received FCC approval to test jamming technology that intercepts and terminates cell phone calls. In one test, South Carolina officials reported that the technology was very effective at jamming cell signals without interfering with cell signals in areas adjacent to the facility. However, the approval to test was for a limited time and the FCC has not granted approval to implement the use of jamming technology.¹⁸ With the growing national concern regarding use of contraband cell phones both as a localized risk and a national security risk, there is renewed interest in seeking prison specific

that didn't pass successfully through the metal screener (purses, coats, belts, shoes) were subsequently carried into the prison without any search or screening.

17 Wireless carriers will permanently disable stolen phones, <http://blog.sfgate.com/pender/2012/04/10/wireless-carriers-will-permanently-disable-stolen-phones/>

18 Special Report, Office of Inspector General “Inmate Cellphone Use Endangers Prison Security and Public Safety”, May 2009

approval for use of jamming technologies.¹⁹ This approach would take into consideration the need to not hinder legitimate communications for administration, guards and others within the confinement areas.

The CCST Project Team recommends that California (via legislative and executive branch efforts) work in coordination with other states and California's federal legislators to seek prison specific exceptions to the Federal Communications Commission (FCC) anti jamming regulations. If such exceptions are provided by the FCC the jamming technology should be tested in one or more pilot projects at California State Prison facilities before implementation.

9. What is Happening Nationally and in Other States?

Federal

The Federal Bureau of Prisons (FBOP) has adopted strict procedures requiring all personnel and materials entering the prisons to be screened by metal detectors without exception. This strict approach to screening all personnel has been implemented to help interdict contraband prior to its entry into the confinement area of their institutions and is reportedly effective. (See Appendix 2 for full policy.)

The Federal Bureau Of Prisons has not yet implemented MAS in their prisons. In September 2011, the U.S. Government Accounting Office (GAO) issued a report²⁰ on Contraband Cell Phone use in Federal Bureau of Prisons institutions noting the size of the issue and recommending that the FBOP should coordinate and share information with the states. Several states were called out (Alabama, California, Florida, Maryland, Mississippi, New York, New Jersey, South Carolina and Texas, as active in the arena of contraband cell phone mitigation studies. The GAO report reinforces that the cell phone issue is a problem and that no one-technology solution can fully address it; the report notes that a combination of detection, managed access and inspection should be considered.

States

The state of Mississippi is the only state known to have a MAS deployed. It has been installed at only one prison, Parchman Prison. This MAS implementation was started in July 2010 and is still not fully operational as of November 2011.²¹ The reasons for this are operational but not provided in detail here at the request of the Parchman Prison administration.

South Carolina is preparing to start a pilot for MAS, Georgia has an RFQ out for MAS and Texas is preparing to issue and RFQ for MAS. Both Georgia and Texas are using the California CDCR IFB as templates for their bid requests. The information availability of correctional facility mitigation techniques in foreign countries is not readily available for public review so the study team was unable to assess if or how well MAS might be working outside the U.S.

10. Review of Managed Access System (MAS) Technology

What is Managed Access?

The Managed Access System (MAS) refers to a standard cell phone network system used in a defined close quarter geographic area such as a campus, military base or a prison. The theory behind MAS is to allow authorized cell phones to connect to the standard carrier (e.g. AT&T, Sprint, T-Mobile,

¹⁹ New Jersey interest (Assembly Resolution 30 (Coughlin), 2011-2012 Legislative Session

²⁰ <http://www.gao.gov/products/GAO-11-893>

²¹ Call with Parchman Prison – Team member Diamond.

Verizon) networks, while preventing unauthorized cell phones from connecting to the carrier networks. A well-designed and implemented MAS would function as a system to detect and preclude the operation of cell phones not authorized in the MAS approved database (Figure 1).

As depicted in Figure 1, the sequence of operational events follows:

1. Within a defined area, the MAS detects a cell phone attempting to connect to its service provider's base station – **A**
2. The MAS decodes the call information to determine the calling cell phone identity.
3. The MAS then compares the decoded cell phone identity to a database to determine if this device is authorized for use within the MAS umbrella of operations.
4. If the cell phone is authorized, the call is allowed to continue uninterrupted by the MAS - **B**
5. If the cell phone is not authorized, the MAS prevents the cell phone from connecting to the carrier's network. Once the MAS has taken control of the cell phone call it can send a pre-designated message to the cell phone stating it is unauthorized for use, or any other message the MAS owner/operator chooses - **C**

This sequence of events is identical to that used by commercial cell phone providers to process calls from cell phones, except for the interdiction and return message for unauthorized calls. All cell phones have to go through an authorization process with the service provider's network database in order for the call request to be processed.

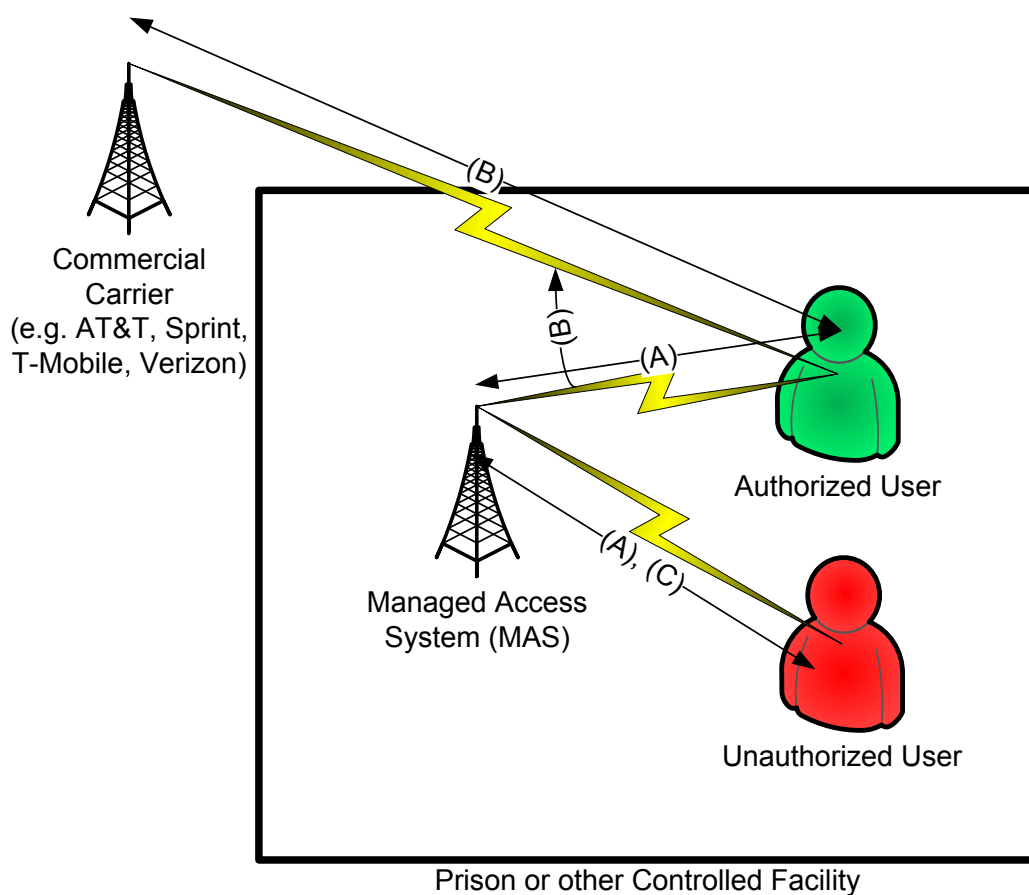


Figure 1. MAS would function as a system to detect and preclude the operation of cell phones not authorized in the MAS approved database

The physical equipment used to develop and operate a MAS is similar to that used by commercial cell phone providers, though on a much smaller scale. Both a MAS and a cell phone provider network are comprised of base station controllers, antenna arrays, interconnect cabling and computers for management and information gathering.

Technical Feasibility of Managed Access Systems

The MAS is essentially a modified implementation of existing cell phone technology. If properly designed and implemented it should be able to block all unauthorized calls within their radio envelope and receiver signal identification capability. **However, MAS can only block calls from cell phones using compatible broadcast technologies.** For example, if a service provider implemented a new service, such as LTE (Long Term Evolution, referred to as LTE and marketed as 4G LTE, is a standard for wireless communication of high-speed data for mobile phones and data terminals) the MAS would not be able to recognize or block phones using the new service. Though the CDCR IFB indicates that it would give the MAS vendor 1-year from commercial availability to incorporate new cell phone technologies into the system, the IFB does not appear to provide a triggering mechanism for the 1-year counter, nor a penalty for failing to do so (or even a reporting obligation). This leaves open the important question of what would be the trigger. Also, it is important to note that as new technologies develop there will be a time lag to identify them and to respond with an upgrade in the MAS ability to detect them. The IFB trigger is also not clear with regard to upgrading or modifying the system to address the evolving technologies.

Managed Access System Vendors and Systems

Data regarding commercially available MAS is scarce. This scarcity can be attributed to the infancy of the MAS marketplace and the early stage of product development. The CCST Project Team identified only two vendors ²²of sufficient size to attempt to develop and implement the MAS for the California State Prison system. There are other vendors of technologies that might be configured for the MAS but they were not considered to have sufficient size or qualifications to be viable enough to include in this report. In addition to these two vendors there are numerous resellers that buy products or services from these vendors to configure and resell for different uses or applications. Shawntec, for example, is a reseller who buys equipment from one of the identified vendors. Shawntec is also the company that provided a “pilot test” of a MAS for the CDCR at the Solano State Prison and the California Medical Facility (two adjacent facilities).

It is key to note that currently MAS systems are not custom designed for use in correctional environments; instead, they are miniature cell phone networks similar to those used by Wireless Service Providers such as AT&T, Verizon, T-Mobile etc., with the potential to be adapted to fit small geographic coverage areas such as a correctional facility. ²³ The systems discussed below are either small cell mobile wireless networks or cell phone test equipment configured to “act” as a managed access system.

One of the vendors that the CCST Project Team talked with offers an intelligent network access controller. This company is a systems integrator using sub-assemblies from a variety of suppliers to build their MAS. The specific MAS component is a software and hardware system allowing the transport of several different cell phone protocols (e.g., GSM, CDMA, LTE) to be carried in one “backhaul packet” connecting to the core of the telephone company’s network. This system is a small-scale cell phone network that operates exactly as a service provider network such as AT&T or T-Mobile. The system does not have any automated means to determine RF envelope dispersal for interference management.

²² Tecore Corporation and DRT Corporation, a wholly owned subsidiary of The Boeing Corporation,

²³ RF envelope and interference management are discussed in Appendix 3

The only MAS system currently implemented in a U.S. correctional facility is the Parchman Prison in Mississippi. This system has been in operation at Parchman Prison since July 2010. According to the Mississippi Department of Corrections, this MAS is still a pilot operation and is not fully deployed due to operational issues. Roll out of the system to other Mississippi prisons is on hold until these issues are worked out satisfactorily.²⁴ The equipment used at Parchman Prison is not the equipment tested in California at a CDCR facility.

Another vendor uses test equipment that emulates the base stations and phones as well as the operational radio network controller function. **This is the equipment that was used by the CDCR in its pilot test of MAS capability at Solano State Prison and the California Medical Facility.**²⁵ In the tests at these two prisons, the subsystems described above were configured to be a MAS capable system. The equipment used did not have any automated means to determine RF envelope dispersal for interference management (i.e., there is no way to determine if the radio signal it generates could or is causing interference outside the confinement area of the prison). The CCST Project Team did not find any evidence that this combination of subsystems was implemented as a fully operational MAS. The CCST Project Team reviewed a copy of the summary report of the CDCR pilot-testing program. Notable in the CDCR summary report was a lack of description of the equipment used or any of the operational issues encountered during the test implementation or operation. Members of the CCST Project Team discussed the test with a CDCR representative who worked with the vendor. **From the discussion, the CCST Project Team learned that the test was very rudimentary and would, at best, constitute a proof of concept, not an acceptable operational pilot test.** The CCST Project Team understands that the tested MAS did provide a cell phone blocking function, but it was not automated. Consequently the MAS experiment was very manpower intensive and never operated in a standalone mode as required by the CDCR IFB.²⁶

Risk and Challenges of the MAS Approach

Because of the paucity of system vendors, the lack of the ability to monitor interference outside of the subscribed area, and the lack of large-scale operational application of technologies used for MAS, there is no template of implementation techniques to model or follow for MAS. If the CDCR proceeds with the IFB as currently written, it would be important to note that **each correctional institution installation will be a new learning experience, and each caveat would be discovered as it is installed.** Although similar problems are likely to arise at each installation, solutions for each individual prison are likely going to vary significantly depending on a complex host of local factors. The proposed MAS systems lack the finite systematic radio power level control capability necessary to prevent interference in real time. This means the only mechanism for interference mitigation would be by exception. For instance, when someone's cell phone service outside the prison is affected by interference, they would need to report it, and the cause could then be detected and corrected. The proposed MAS approach also lacks the capability to be simply modified for new cell phone communications technologies. Each and every upgrade of the MAS systems will be tantamount to a complete new installation. This, predictably, would be disruptive and could lead to long periods of inferior performance.

Still, the concept of utilizing MAS to control cell phone use in prisons is an appealing concept. Some of the many challenges that need to be addressed to have a fully functional and effective system include:

²⁴ This information was collected in telephone contact with Mississippi corrections management in November 2011 by CCST and California Senate Office of Research individuals.

²⁵ Information on this pilot provided by CDCR.

²⁶ As conveyed by CDCR personnel to the CCST Project Team.

Frequency Allocation

The MAS uses a licensed radio spectrum owned by the service providers, (e.g. AT&T or Verizon), and therefore it is illegal to “radiate” in these frequencies without prior agreement with the spectrum owners. The spectrum owners are under no obligation to allow free use of this radio space to the prisons or to agree to any for fee use for deployment of the MAS. The CDCR has stated they will lease the spectrum from the spectrum owners and through re-lease agreements; the MAS operator will utilize the spectrum. **While this approach could ensure the spectrum is available for MAS it will not absolve the CDCR from interference liability, and may in fact make CDCR liable for interference. This approach increases the requirement for tight control of the RF envelope dispersal.**

FCC Regulations

Relatedly, the lack of an FCC requirement for spectrum license owners (e.g. Verizon, AT&T, etc.) to allow for use of their spectrum within the prison area to be used for MAS is a key issue. Without this requirement, the state is forced to negotiate with each carrier on its own to enable the MAS operation. To date, the FCC has not created a policy for corrections departments at any level to acquire the permission from the spectrum owners for ways to control the calls (e.g. MAS or jamming). **A coordinated effort of several states to petition the FCC to modify existing spectrum owners’ agreements to require they provide unobstructed use of their spectrum within the geospatial confines of corrections facilities would be an important modification of regulations. If this effort is undertaken, the discussions could also include the possibility of using jamming technologies in some conditions.**

Installation

Since the MAS is a cell phone system with antennas and interconnect cabling and support computers it will need to be installed in highly secure areas away from inmate access to prevent tampering or destruction. **The existing cabling systems in prisons will not support the RF signaling being carried to and from the antenna arrays and the transmitter receiver systems. All required MAS infrastructure will need to be newly installed.**

RF Dispersion

Since the MAS radiates RF energy capable of interfering with any cell phone using the same frequencies, absolute control of the RF envelope is mandatory. The RF envelope is the actual physical distance and pattern that the RF energy travels and the dispersal power of the radiated energy. In simple terms, this means the MAS system’s radiated energy cannot be allowed to propagate beyond the specific physical confines of the prison area. This RF envelope will change characteristics with temperature and humidity, wind, tree growth and building construction or modification. The complexity and negative effects will vary by prison location. For example, a prison in a highly rural area may be far enough away from roads or structures that RF leakage would be an issue only when someone entered into the prison MAS “zone”. **However, if the prison is in or near a populated area, this RF leakage could be highly disruptive to cell phone usage by the non-prison population. Among other things, this disruption could greatly reduce the capability of public safety professionals to serve the community’s needs or the general public’s ability to access a 911 operator.**

The control of the RF envelope is the combination of signal transmission power and antenna output lobe dispersal management. **Ideally, the MAS would have a dynamic signal power and direction control system capable of changing the output signal based upon the immediate environmental circumstances.** This dynamic system would be comprised of what are called active feedback sensors to measure the specific energy emitted by the MAS antenna. These sensors would then provide real time feedback to either the MAS to automatically change power of energy emitted or more realistically notify the MAS operator of a need to correct any RF leakage outside the target coverage

area. The construction of each prison and its location in the population demographic will mandate that the MAS implementation technique and RF envelope management be employed.

11. Limitations of Managed Access System Technology

The basic capability of the proposed MAS equipment to recognize cell phone usage in all the current bands and modulation techniques, e.g., CDMA, UMTS, GSM, and block or interdict the call is available today. The capability to detect and interdict 4G signals such as Long Term Evolution (LTE), however, is not currently available. It is expected that a MAS vendor would need to implement LTE radio interdiction prior to implementation of the MAS. This capability is fundamental to cell phone network system operation and should not be technologically challenging.

However, in the context of the current CDCR IFB and the requirements for RF envelope control for interference mitigation coupled with highly automated operation, neither of these above approaches would be classified as effective. Current MAS technologies require significant human intervention and operational action due to a complete lack of automated feedback of operational performance. The MAS systems of today cannot distinguish the location of a cell phone for blocking. If the RF envelope is incorrectly deployed, all cell phones in its range will be blocked unless specifically identified as an allowed user on the access control list. The IFB calls for all 911 calls to be allowed to pass. It is important that all emergency calls be routed to the E911 Emergency Response Center and not to another location coded into the MAS call routing system.

Circumventing the MAS

The idea of circumventing the MAS is more of a use case question than a technological question. If the MAS is capable of identifying that a cell phone is in use it can interdict and block the call. However, as different applications of the 'cell phone' or Wi-Fi connectivity are developed, it is likely that the MAS could be bypassed.

Texting

Texting is a simple means to send a brief "note" from one cell phone user to another, analogous to a Post-it note. The sender types the message and then pushes the send button. The message is sent immediately to their service provider, who stores it for future delivery to the recipient. This is very different from a voice phone call, in which the service provider must actually locate and connect to the targeted user before the call is processed. Text messages take less than 1 second to send; in comparison, it takes up to 5 seconds to establish a connection for a voice call.

The time difference is important because the IFB for the MAS requires that the system detect and attempt to block unauthorized calls within 60 seconds; this could result in the response time being the full 60 seconds. Inmates will figure out that a text message can be sent in seconds and does not require the cell phone to "dial a phone number" as with a voice call. A text message can even be prewritten offline, and the cell phone activated and the message sent in well under the 60 second requirement of the IFB for the MAS to detect the attempt and block its completion. Because texts can be sent very quickly, the efficacy of the MAS in blocking these has not been proven. The receiving cell phone of a text can even be turned off when the text is sent because the network will store and forward the text message when the receiver's phone is turned on.

Incoming Calls

One more area of concern is the MAS efficacy in blocking incoming calls to contraband cell phones, especially for text messages. It is not known what would happen if the MAS attempts to block a service provider base station; in this case, the contraband cell phone is not attempting to place a

call. It is hypothesized that incoming calls would also be processed much faster than a call out and thus may circumvent the 60 second window for the MAS to activate. This scenario has not been tested.

Data Transmission via Flash Memory Card

Most cellular phones available today have the capability to read and write to small flash memory cards. The most common flash memory used today is the microSD card, which is as small as a thumbnail – microSD cards measure only 11mm x 15mm. (See Figure 2.) This small memory card can hold as much as 64GB of data today, and will only increase in capacity in the future. By utilizing flash memory cards, inmates could send text files or images both inside and outside of the prison walls, simply by saving files onto the card and physically distributing the small device.



Figure 2: Flash Memory microSD
Card Image from <http://support.jvc.com/consumer/products/glossary.jsp?gld=337>

12. Can California Serve as a MAS Model?

The CDCR has stated the desire to be the model for effective contraband cell phone interdiction efforts for the United States. Given the state of implementation nationwide, if installed and implemented, the CDCR would be the test case for the first large scale MAS deployment. The CDCR has an aggressive schedule for MAS deployment for 33 institutions in 36 months. The plan is to implement the first site in Solano State Prison to gain “acceptance” before proceeding to phases 1 and 2, which effectively split the 33 target institutions into 2 groups²⁷. If contraband cell phone use interdiction is mandatory, some form of cell phone MAS could be useful. However, the current MAS technology designs need more testing to understand the rigors of a correctional institution environment.

²⁷ Invitation for Bid (IFB) was issued by the California Technology Agency on behalf of CDCR on July 7, 2011; IFB 11-126805

Review of California Department of Corrections and Rehabilitation (CDCR) Pilot Program Findings and Conclusion

Members of the CCST Project Team reviewed available CDCR documents about their MAS pilot effort and discussed the test effort with the CDCR staff. The CCST Project Team concluded from available information that the MAS test was more a proof of concept demonstration rather than a true pilot MAS installation. The CCST Project Team also concluded that the proof of concept effort undertaken by the CDCR was not robust enough to form the only basis for the technical content of the CDCR IFB. The Project Team learned that in the case of the data showing “successful” call blockings, the vendor supplied the cell phones; furthermore, only one cell phone of each service provider type (e.g. AT&T, Verizon, etc.) was tested. The test lasted a total of 96 hours (4 days). This does not constitute a suitable test period for a system with the complexity of the MAS that is proposed to be deployed across facilities of different designs with varying geographical and weather parameters.

Missing Financial Documentation and Efficacy Requirements in the IFB

The CDCR IFB is written so as to require the winning bidder to operate, maintain and pay all costs associated with the MAS. The MAS is to be funded from revenues generated by the Inmate and Wards Telephone System (IWTS) operation. This system is provided to incarcerated persons by the CDCR but operated and maintained by a third party vendor. The IFB for the MAS is a portion of a greater IFB including the IWTS and MAS systems. The IFB calls for a portion of the revenues from the IWTS operation to be used to implement, operate, and maintain the MAS with no cost to or use of CDCR resources. The IFB calls for the winning IWTS bidder to pay the CDCR \$800,000 annually for 6 years with a CDCR option to extend the contract for 4 additional years. Beyond training that some CDCR personnel will receive to enable use of the MAS database and management of the proposed trouble ticketing system, full responsibility for the installation and operations of the MAS belongs to the winning bidder. It was not clear from the documents reviewed how the \$800,000 payment amount was calculated and what it is based upon; thus it is not clear if this is appropriate or what amount of overall revenue will be generated by the ITWS. One significant concern of this proposed arrangement is the issue of how to measure success at the corrections facilities included in the IFB. There is no mechanism in the IFB requirements that provide for third party (or even CDCR) evaluation to determine if the system is working or to adequately adapt the system to changing technologies or other circumstances.

Societal Considerations

The societal considerations for the MAS in corrections facilities are broad and varied. In CCST’s initial review of the July 7, 2011 IFB from CDCR, there was noted concern that information collected during the process of blocking contraband cell phone calls could be covered by a variety of privacy laws. In subsequent IFB revisions, the categories of data collected during a blocking activity by MAS have been significantly limited. These changes eliminate CCST’s concern that collected data was potentially a privacy issue.

During CCST’s visit to two prisons (Solano State Prison and California Medical Facility) in January 2012, we had the opportunity to interview inmates, gathering a unique perspective on the contraband cell phone issue. The opinion expressed by some inmates during those visits was that cell phones used by prisoners allowed unfettered contact to family and loved ones otherwise unavailable. The question, “If cell phones were provided as part of the IWTS, and knowing that the calls were recorded, would this deter cell phone use?” was answered with a “no”; the inmates indicated that they were used to their calls being recorded when using the IWTS. There was also acknowledgment by the prisoners that a percentage – small by the inmates’ estimation – of cell phone calls are used for illicit and illegal activity. It was noted by the CCST Project Team that access to cell phones (even if monitored by CDCR via computers with screening software) offers to many inmates an ongoing

connection to family and friends, as well as entertainment on smart phones (such as games, videos and ESPN sports games). Consideration could be given to piloting a method to screen contraband cell phone calls (rather than blocking) to better understand the impacts that the phones have on prisoner recidivism and overall prison temperament.

13. Benefits of a Robust Pilot Project

With regard to the MAS, CCST's overall findings are that the MAS technology of today is not yet mature enough for large-scale deployments such as the 33 CDCR prisons target. In addition, the CDCR has not actually identified the size of the problem or a mechanism to determine the efficacy of MAS deployment to mitigate contraband cell phone usage. CCST recommends a delay in deployment of the CDCR MAS for a period of 18 months to enable a robust MAS Pilot Network installation and operation that could be designed to address the following set of issues:

Establishment of a baseline and development of measures of efficacy:

No specific measurable target of efficacy for the MAS has been identified in the IFB with regards to the volume of cell phone usage before and blocked calls after the MAS deployment. The pilot network installation needs to include a means for determining the "size of the problem on a per institution basis."

An accurate measurement of the problem needs to be determined in advance of implementation of the MAS to establish a baseline "size of the problem" for each institution. The CDCR has no baseline of the actual volume of calls originating from contraband cell phones over an extended period of time. The only metrics existing are the number of cell phones confiscated and a measurement of calls attempted during the 11-day test at Solano State Prison. An accurate and current baseline is important to determine the efficacy of the MAS.

To obtain this baseline measurement, cell phone RF detection equipment would be placed throughout the target facility and configured to achieve 100% coverage, for 30 days immediately prior to the MAS installation. The detection equipment would need to capture the cell phone identifier²⁸ of the device placing the call so authorized calls would be filtered out prior to the MAS target metric establishment. The exact settings of this capture equipment would need to be studied since the potential for calls placed in very close proximity to, but outside the confinement area would need to be excluded. Also, close coordination with the local wireless service providers would be necessary.

Development of a template for implementing the MAS in a correctional institution:

There is no proven template for implementing the MAS in the demanding environment of a correctional institution. The pilot network installation will result in creation of this template. The MAS as a unique technology solution to blocking usage of contraband cell phones in prisons has yet to prove itself as successful or unsuccessful.

With only one installation in a uniquely rural prison (Parchman Prison in Mississippi) started in July 2010 and still unproven, the jury is still out on the ability of this approach to be applicable to the prison environment. It is clear that MAS technology would be able to block cell phone usage in a controlled environment. It is not yet clear that this technology can be effectively installed and operated in a prison facility. Also of concern is whether the unproven system could be effectively managed by the CDCR and the successful IWTS/MAS vendor. A true pilot MAS system needs to be tested before being adopted by the CDCR. An effective pilot MAS should be tested for 9 to 12

²⁸ It is unclear whether this is legal or not. The CCST Project Team received various answers from vendors, law enforcement and lawyers.

months. This pilot implementation needs to be “live” and block contraband cell phone usage as intended in the IFB. This pilot could become the “template” for subsequent MAS implementations in the CDCR and potentially all U.S. state and federal correctional institutions deemed appropriate for MAS. This is not a trivial task.

[Establishment of a third party oversight and verification of effectiveness:](#)

No ongoing third party oversight or review of the MAS operation and conformance to wireless operations standards is addressed in the IFB. This issue could be addressed in a pilot with a mechanism for third party oversight being developed during network installation and operation.

This would be a detail-oriented process to ensure things such as the MAS being in compliance with the FCC regulations. This would also allow for refinement of agreements with local mobile wireless operators and identification of a third party to assure efficacy.

[Development of a process to ensure the MAS evolves to address emerging technologies:](#)

There is no mechanism to measure vendor compliance to emerging wireless technology and deployment modernization techniques. These mechanisms will be devised and the process documented during the pilot network installation and operation.

This is a longer-term process of identification of new wireless technology inclusion into the MAS by the operator and verification of operation and efficacy by the CDCR.

[Review of societal issues related to cell phone use by prisoners:](#)

A pilot project would afford the opportunity to consider if there are some positive aspects of cell phones in the prison environment (perhaps in minimum security facilities) such as staying connected to family and friends and to relieve boredom (e.g. watching ESPN). The pilot would also provide a chance to evaluate the impact of eliminating cell phone access on the overall state of mind and behaviors of inmates, both individually and throughout a facility. This is not a technological or operational issue. This concerns the state of mind and behaviors of inmates. The pilot project could experiment with options such as allowing some cell phones that are provided with the understanding they would be monitored and recorded similar to the IWTS.

14. Third Party Consortium Oversight

The issue of contraband cell phones in prisons is very complex. Entrance detection, correctional personnel education, inspection and MAS combined has the potential to be effective if the MAS system is tested and modified to be effective in the prison environment. A thorough study of the MAS combined and with the communities of interest has the potential to develop into a successful mitigation method.

A consortium of participants should be identified and tasked to develop the pilot parameters and specifications, and to oversee installations, operation and evaluation. This same consortium would oversee and obtain the baseline measures needed to determine the efficacy of the pilot and to help determine return on investment (ROI) with regard to the MAS interdiction approach. Members of a consortium could be drawn from independent experts, the CDCR, California Senate Office of Research (SOR), the California Technology Agency (CTA), the University of California (possibly the UC Center for Information Technology Research in the Interest of Society (CITRIS) and UC California Institute for Telecommunications and Information Technology (CalIT²), the California State University (CSU) system, relevant local mobile wireless service providers, the Cellular Technology Industry Association (CTIA), the Federal Bureau of Prisons (BOP), the Federal Communications Commission (FCC), and the American Correctional Association.

This consortium could design and implement one or more pilot MAS efforts and could study the technological nuances found in correctional institutions that might impair effective installation of the MAS, the impacts on prisoner attitudes and behavior to a dramatic loss of outside world contact, the long term issues of effective installation, maintenance, and operation, and the legal implications on inmate privacy. The consortium would be able to expand upon this initial list.

A successful pilot approach could become the template for regulatory, societal, legal and procedural process and actions for use of MAS on a national scale.

The consortium could also take an in-depth look at alternative options for mitigating contraband cell phones such as the screening technologies, use of microcells, and exploration with cell phone carriers for their engagement in denying services to unregistered cellular phones seeking connection from within prison confinement areas.

Appendix 1: Project Team Members

The CCST Contraband Cell Phones in Prison Project is fortunate to have an outstanding set of participants led by Charles Harper.

Chair

Charles Harper, Senior Vice President, Strategy and Systems Innovation Group, Semtech*

Technical Experts

Patrick Diamond, Consultant & Technical Project Study Team Lead

David Goldstein, Sr. Systems Engineer, The Charles Stark Draper Laboratory, Inc.

Brian W. Carver, Assistant Professor, University of California, Berkeley

NASA Ames Technical Experts

S. Pete Worden, Director, NASA Ames Research Center**

Don Beddell, Network Engineer

Bobby Cates, External Interface Network Engineer

Deb Feng, Deputy Center Director (acting)

Ray Gilstrap, Network Engineer, Information Technology Directorate

William Hunt, RF/IT Technician

William Notley, ARC RF Spectrum Manager

James Williams, IT Director and ARC Chief Technology Officer

CCST

Susan Hackwood, Executive Director

Lora Lee Martin, CCST Director, Sacramento Office

* CCST Board Member

** CCST Council Member

Appendix 2: CCST Letter to Senators Identifying IFB Issues of Concern (October 29, 2011)



CALIFORNIA COUNCIL ON SCIENCE AND TECHNOLOGY

Sustaining Members

University of California • California State University
California Community Colleges • California Institute of Technology
Stanford University • University of Southern California

Laboratory Affiliate Members

Lawrence Berkeley National Laboratory
Lawrence Livermore National Laboratory • Sandia National Laboratory
Stanford Linear Accelerator Center • NASA Ames • Jet Propulsion Laboratory

Friday, October 28, 2011

Senator Elaine Alquist
Senator Loni Hancock
Senator Christine Kehoe
Senator Alex Padilla

Subject: Contraband cell phones in California prisons; initial response your July 7, 2011 request of the California Council on Science and Technology

Dear Senators,

The California Council on Science and Technology (CCST) received your July 7, 2011 request for a study of the technologies related to managed access of contraband cell phones. The request has been reviewed by the CCST Board and Council and we have received their approval to proceed.

A team of technical experts has been convened (see attachment A) to do a thorough review of the technologies involved. In the process of reviewing background material, the project team raised serious questions related to the California Department of Corrections and Rehabilitation's Invitation for Bid (IFB). It is our understanding that the deadline for submission of responses to the IFB is Monday, October 31, 2011. Given this deadline and the urgency of the issues raised by the team, we write to bring them to your immediate attention. The CCST project team recommends that these issues be clarified and addressed, and that the CCST report be completed prior to awarding a contract to the winning bidder.

The types of issues identified include those that have the potential to provide both financial and liability risks to the State. A preliminary list of issues is provided as attachment B. We would be happy to convene a subset of the project team to meet with you to discuss each of these in more detail.

The CCST project team withholds its technical opinion as to whether a MAS approach is the best approach for all (or some) of the prison installations to eliminate contraband cell phone use. In the CCST report the project team will provide an analysis of the MAS approach as well as explore alternative ways in which contraband cell phones might be addressed. It is our intent to provide you with a preliminary draft report in December and a final report at the end of January.

Sincerely,

Charles Harper
Chair, Contraband Prison Cell Phone Project
CCST Board Member

Susan Hackwood
Executive Director
California Council on Science and Technology

Cc: Mim John, CCST Council Chair
Peter Cowhey, CCST Council Vice Chair
Karl Pister, CCST Board Chair

Attachments:

- A. Contraband Cell Phone Project Team Members
- B. Preliminary List of Issues Identified

1130 K Street, Suite 280, Sacramento, CA 95814-3965
Phone: (916) 492-0996 • Fax: (916) 492-0999 • E-mail: ccst@ccst.us • Web: www.ccst.us

Attachment A

Contraband Cell Phone Project Team Members

Chair

Charles Harper, Senior Vice President, Strategy and Systems Innovation Group, Semtech

NASA Ames Technical Advisors

S. Pete Worden, Director, NASA Ames Research Center

Deb Feng, Deputy Center Director (acting)

James Williams, IT Director and ARC Chief Technology Officer

Bill Notley, ARC RF Spectrum Manager

Bill Hunt, RF/IT Technician

Bobby Cates, External Interface Network Engineer

Don Beddell, network engineer,

Ray Gilstrap, network engineer, Information Technology Directorate

Other Technical Experts

David Goldstein, Sr. Systems Engineer, Draper Laboratory

Pat Diamond, Consultant

CCST

Susan Hackwood, Executive Director

Lora Lee Martin, Director Sacramento Office

Attachment B

California Technology Agency - Invitation for Bid Preliminary List of Issues Identified

Overview - Managed Access System – Invitation for Bid

The California Department of Corrections and Rehabilitation (CDCR), via an Invitation for Bid (IFB), have requested proposals for the development of a Managed Access Systems (MAS) for the California State Prisons. Submissions must be received by close of business on October 31, 2011. As described in the IFB, MAS is a technology system made up of several elements including cell phone use detection within the confines of the correction facility boundaries, a comparison of cell phone use with a list of those authorized, interruption of cell phone calls to the wireless service provider base station, and recording of these events in a computerized database for reporting purposes. The MAS is intended to automatically prevent the unauthorized cell phones from working without consumption of correction facilities resources.

The CCST study group has reviewed the IFB in detail and has identified points the committee feels warrants more detail or clarification. Those points are listed below. Of particular note, there is no mechanism required to ensure efficacy of the system once in place. In the IFB the metrics requested include: system availability, number of legitimate calls denied by the system, and amount of acceptable signal degradation to the emergency responder frequencies. There is no mention of an acceptable percentage of contraband attempts denied or a method to calculate such a number. Also, interestingly, there is no cost to the State for the MAS. In fact, the vendor will provide to the state \$800,000 annually over the life of the contract as an administrative fee (sec 6 of the IFB). The vendor will make their returns from the landline telephone service that provides communication between the families, lawyers, and inmates. The project team raised the question, "will the landline revenue be enough to keep the MAS systems current and effective while maintaining calling rates that are fair and reasonable?" As in all things there will be a cost/benefit decision. It would appear from the IFB that the vendor will be the one making the decision as to what is cost effective. Which may not necessarily be in the State's interests.

It is important to note that CCST has not yet undertaken any independent technology evaluation concerning the veracity of MAS as a solution but a detailed report is being created.

The issues, below, are presented in order of priority:

Items with direct risk to the State

1. **Lack of requirement for agreements with spectrum owners: It is a violation of Federal law to use licensed spectrum without permission of the registered owner.** A requirement for the winning bidder to coordinate, communicate, or secure an agreement with the current (or future) owners of any licensed spectrum that will be necessary to access for the system to be effective is not in place. Lack of such an agreement may create a liability for the state.

2. **Data ownership and confidentiality:** If this system is hacked it could lead to personal safety risks and privacy of communications issues. The IFB states that the bidder will be the “owner” of all data collected by the MAS. The requirement for data confidentiality is clearly stated in the IFB. To help ensure the confidentiality of the data, should the owner of the data be the State? What will the chosen vendor do with that data other than store it? The IFB further includes a requirement that includes access for CDCR personnel to inspect and review the data. The only requirement noted for data encryption is when it is moved via an external media such as DVD. There is no requirement for encrypting the data stored in the system.
3. **Potential liability exposure with expansion of purpose from blocking to snooping:** This could lead to a violation of the prisoners right to due process and attorney client privilege. The MAS is required to not only block unauthorized access but also have the capability to “snoop” on the communications of a cell phone upon CDCR warrant. This may become a privacy issue that could create a liability for the State. For instance, if this includes communications with an inmate’s attorney, it might be privileged information.
4. **Security of the MAS information technology technologies:** If this system is hacked it could lead to personal safety risks and privacy of communications issues. This could lead to a violation of the prisoners right to due process and attorney client privilege. The IFB does not address, nor does it require the bidder to address, the in prison security required to ensure that the integrity of the MAS cannot be tampered with or disrupted by inmates or other personnel in the prison environment. This includes both interception of information from the MAS as well as overall integrity of the MAS system.

Items affecting system efficacy

5. **Lack of 3rd party verification of effectiveness:** This could lead to a system that does not meet the requirements of the CDCR. The IFB provides that the bidder will be responsible for testing and reporting on the MAS System and Carrier Signal Verification. Said another way, the winning bidder will be the one responsible for telling CDCR and the state if their system is working. There is no provision for having this validated by a third party. There is no clearly stated “audit” mechanism for the state to insure MAS is actually blocking calls by unauthorized cell phones.
6. **Unreasonable requirements for future spectrum band management:** This places an unrealistic technological obligation on the MAS for future proofing of technology as yet undefined. The IFB lists the radio frequencies of operation to be used by the MAS. It further includes a requirement that other spectrum bands that will potentially be used for cellular communications in the future be included in the capabilities of the MAS. This is technically challenging, as is the need to determine who will own those bands and what access will be available.
7. **Lack of mechanism to ensure the MAS provider does not interfere with authorized cell calls.** The MAS could be interfering with signals outside the perimeter of the correction facility relating to public safety and emergency response. This mechanism would ensure that the MAS and any service provider “airwaves” are operating coherently on a facility-by-facility basis. It is important that the frequencies of the service providers do not interfere with the MAS and vice versa with regard to authorized cell calls. This is a necessary technical issue to make sure that authorized calls will be functional. Per the

IFB, the MAS system provider is responsible for determining the service provider's signals and that the MAS and IWTS can both survive (not interfere) in this dual environment. There does not appear to be a verification mechanism nor is there a penalty if the provider fails to do so.

8. **Lack of clearly defined criteria:** This is a requirement without a measurable endpoint. The IFB requires that the MAS must be fully deployed and operational 18 months after the winning bidder is notified. However, there is no clear set of criteria to determine what "fully deployed and operational" means.
9. **Lack of attention to work-around technologies:** This places an unrealistic technological obligation on the MAS for future proofing of technology as yet undefined. The IFB narrowly looks at current cell phone technologies without building in requirements for the bidder to ensure that their MAS will be evolving to capture signal from work-around technologies such as intercepting or blocking calls made via an internet connection such as Skype, satellite phone technologies, or other technologies yet to be invented. The IFB provides for a six-year contract with possible extension for another four years. Ten years will see significant evolution in communication technologies that could easily outstrip the capabilities of any technological solution defined today.

Items affecting practicality/capability

10. **Lack of access to existing wiring infrastructure:** This requirement could disqualify otherwise capable bidders from participating and does not seem to have a basis or reason. The winning bidder is required to install at no cost to the state, the physical infrastructure necessary to operate the MAS, including but not limited to wiring systems hardware. The IFB specifically excludes the use of any existing wiring facility. Why is this existing infrastructure not accessible? What will it be used for? Without this restriction the universe of potential bidders may be expanded beyond the limited MAS vendor community.
11. **Cost of the MAS vs. land line revenue:** These does not appear to be a remedy for the bidder if the revenues from the IWTS fail to adequately cover the costs of operation of the MAS. The IFB notes that the selected vendor will install the MAS at no cost to the State. In fact the vendor will provide to the state \$800,000 annually over the life of the contract as an administrative fee (sec 6 of the IFB). In return, the selected vendor will be given the land line telephone communication business to all the California State Prisons with an expected 99.7 million minutes of prepaid call time at a rate to not exceed \$0.15/minute. This raises two questions: why won't existing wiring infrastructure be used, and what are the assurances that the price of calls on land lines will fully cover the cost of the MAS system installation and operations without overburdening the cost of these calls?
12. **Weight of IFB focused on inmate warden telephone system not MAS:** The MAS system appears to have been an afterthought and the lack of precision in its requirements could lead to a failed system implementation. The preponderance of detail and information in the IFB is focused on the IWTS not the MAS. Many of the issues noted about would have been expected to be in a more detailed MAS IFB. The IFB appears to have added the MAS at the end of the document without the same careful detail as the IWTS requirements.

Appendix 3: Letter from Senators to Matthew Cate, Secretary, California Department of Corrections and Rehabilitation (CDCR) Conveying Issues from CCST's October 2011 Letter

CALIFORNIA LEGISLATURE

STATE CAPITOL
SACRAMENTO, CALIFORNIA
95814

November 6, 2011

Matthew Cate, Secretary
California Department of Corrections and Rehabilitation
1515 S Street,
Sacramento, CA 95814

Dear Secretary Cate:

Please find enclosed a preliminary report from the California Council on Science and Technology (council) on the California Department of Corrections and Rehabilitation's (department) proposed managed access program.

The council was requested by the signatories of this letter to study the technologies related to managed access of contraband cell phones.

The department's managed access program is a potentially innovative way of blocking illegal cell phone use by department inmates. However, by relying on a unique technological solution there is significant initial and ongoing risk that could impede successful implementation.

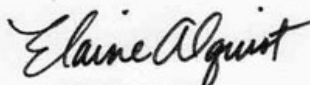
The council will produce a draft report in December 2011 and a final report on February 1, 2012. The council assembled an impressive team of experts and identified issues of concern as the department implements its managed access program. To that end, the council is available to meet with the department and the California Technology Agency to discuss its initial findings.

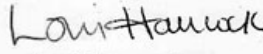
We strongly encourage you to immediately contact the council and avail yourself and your staff of the council's technical expertise. Please contact Susan Hackwood, Executive Director, California Council on Science and Technology, 1130 K Street, Suite 280, Sacramento, CA 95814-3965, 916-492-0996. You can contact Ms. Hackwood or Lora Lee Martin via email at Hackwood@ccst.us or Loralee@ccst.us.

We are supportive of all department efforts to block the use of contraband cell phones by department inmates and to improve safety for department staff and the public. We think the council has identified issues that will help the department as it considers the best way to implement its managed access program.

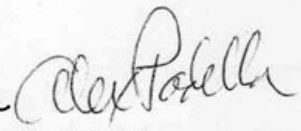
Page 2
Matthew Cate

Sincerely,


Elaine K. Alquist


Loni Hancock


Christine Kehoe


Alex Padilla

cc: Carlos Ramos, Secretary, California Technology Agency

Enclosure

Appendix 4: Preliminary List of Issues Identified with Status Update

Summary of Issues identified by the CCST Project Team in IFB#11-126805 as issued by the California Technology Agency on behalf of CDCR (July 7, 2011). These issues were provided to State Senators in a Letter dated October 27, 2011, and subsequently forwarded by the Senators to Secretary Cate of CDCR (November 6, 2011)

Issue #	Issue of Concern	Summary	CDCR Action Taken	Status
Item of Direct Risk to the State				
1	Require Agreement with Spectrum Owners	It is a violation of Federal law to use licensed spectrum without permission of the registered owner (e.g. a vendor like Verizon).	CDCR modified IFB to take responsibility for licensed spectrum usage agreement	Mitigated in the IFB but still a task to be done.
2	Data Ownership & Confidentiality	If the data resident in the MAS system is compromised it could lead to personal safety risks and privacy of communications issues.	CDCR removed from the IFB the requirement to capture and store information with a privacy component.	Mitigated in the revised IFB
3	Potential Liability exposure with expansion of purpose from blocking to snooping	This requirement in the IFB could lead to a violation of prisoners' rights to due process and attorney client privilege.	CDCR removed from the IFB the requirement to "snoop" on calls.	Mitigated in the revised IFB
4	Security of MAS information technology technologies	If system is hacked, and data resident on system compromised, it could lead to personal safety and privacy issues.	CDCR removed from the IFB the requirement to capture and store information with a privacy component.	Mitigated in the revised IFB

Items Affecting System Efficacy				
5	Lack of 3 rd Party verification of effectiveness	IFB provides for bidder to be responsible for testing and reporting on the MAS System and Carrier Signal Verification.	No Change to IFB evident	Open Issue- no clearly identified audit mechanism
6	Unreasonable requirements for future spectrum band management.	Unrealistic technological obligation on the MAS for future proofing of technology as yet undefined.	No Change to IFB evident	Open Issue

Issue #	Issue of Concern	Summary	CDCR Action Taken	Status
7	Lack of mechanism to ensure MAS provider does not interfere with authorized cell calls	MAS could interfere with signals outside of the perimeter of the correctional facility with a potential impact on public safety and emergency response.	No Change to IFB evident	Open Issue
8	Lack of clearly defined criteria	The IFB requires MAS be fully deployed.... There are no set criteria against which this can be determined.	No Change to IFB evident	Open Issue
9	Lack of attention to work-around technologies	No requirement for MAS vendor to evolve their system to capture signal from work-around technologies	No Change to IFB evident	Open Issue

Items Affecting Practicality/Capability				
10	Lack of Access to existing wiring infrastructure	Winning bidder required to install new infrastructure and excludes use of existing wiring; could disqualify otherwise capable bidder	No Change to IFB evident	Open Issue Potentially a facility specific issue.
11	Cost of the MAS vs. land line revenue	Appears to not be a remedy for bidder if revenues from the IWTS land line fails to cover costs of MAS	No Change to IFB evident No	Open Issue Financial Issue/ exposure
12	Weight of IFB focused on IIWTS not MAS	The MAS requirement was not fully integrated into the IFB but rather appears to be appended on as afterthought. Lack of precision in requirements could lead to failed implementation.	No Change to IFB evident	Open Issue

Appendix 5: April 11, 2012 Letter from Senators to Secretary Cates, California Department of Corrections and Rehabilitation (CDCR) Conveying Notice of the Immanence of the CCST report.

CALIFORNIA LEGISLATURE

April 11, 2012

STATE CAPITOL
SACRAMENTO, CALIFORNIA
95814

Mr. Matthew Cate, Secretary
Department of Corrections and Rehabilitation
Office of the Secretary
1515 S Street
Sacramento, CA 95814

Mr. Gareth Elliott, Legislative Secretary
Office of the Governor
State Capitol, First Floor
Sacramento, CA 95814

Dear Secretary Cate and Mr. Elliott,

We are writing to notify you of the availability of the preliminary results of the study conducted by the California Council on Science and Technology (CCST) regarding the use of managed access system (MAS) technology to prevent the use of contraband cell phones in California prisons. The study was commenced at the request of the signatories of this letter pursuant to a letter dated July 7, 2011 (see Attachment).

The MAS is a potentially innovative way of blocking unauthorized cell phone use by prison inmates. However, by relying on this unique technological solution, both positive aspects as well as potential risks exist related to this proposal. Notable aspects of the proposal:

- MAS will block a percentage of cell phone transmissions. However, the total number of attempted calls (baseline) has not been determined. As a result, the percentage of calls that will be captured is unknown. The number of captured calls will be dependent upon the technology of the phones, the technology/design of the MAS installed, and the MAS implementation technique.
- The potential implementation cost of \$1 million per prison may be accurate.
- There are no front-end General Fund costs required for set-up/installation and first-year implementation. The MAS will likely require human resources costs. The MAS will be financed through foregone revenue from the Inmate/Welfare Telephone System (IWTS) contract to be transferred to the selected MAS vendor.

Potential issues that could impede successful implementation of MAS:

- It appears the MAS is configured based on a MAS being installed in one Mississippi prison which is having implementation and operational problems.
- What is happening to the percentage of cell phone calls not being captured is unknown. As noted above, in the absence of a baseline number of calls, the number of calls not

captured is unknown.

- MAS could result in unintended interruption of civilian/government communications, resulting in significant liability to the state and public safety risk.
- MAS cannot capture Wi-Fi, Mi-Fi, Skype or satellite transmissions or, most importantly, text messages, as currently bid. If specifically designed and properly implemented with text messages in mind, MAS could likely block texts.
- MAS cannot "triangulate" thus limiting effectiveness in identifying cell phone use locations.
- The existence of other workarounds (i.e., SIM card transfer of information) would be another method of transmitting information without detection.
- A more comprehensive MAS may increase the cost of the system. Actual costs will not be clear until determined/refined by one or more pilots. "CDCR needs to implement 33 cell phone networks."
- At this time, system economics, i.e., the cost of initial system and technology upgrades required by the contract versus land-line revenues are uncertain.
- CCST has identified only two vendors nationwide at this time who offer MAS (not an exhaustive search).
- MAS will not be a complete solution to the problem.

In summary, because the scope of the problem has not been determined, it is unclear how goals will be set or what metrics will be used to determine success. As a result, the expected cost and the overall efficacy of the MAS cannot be determined with confidence at this time.

In advance of the release of the final report, we would like to invite you to a short presentation by the CCST of its findings and provide you with an opportunity for discussion. The CCST has also offered to provide a more comprehensive, formal presentation, for you and your representatives, as well as interested staff from the Department of General Services and the California Technology Agency, upon request.

Please contact Bob Franzoia, Staff Director, Senate Committee on Appropriations, at your earliest convenience to schedule a briefing at 916-651-4101, or Bob.Franzoia@sen.ca.gov.

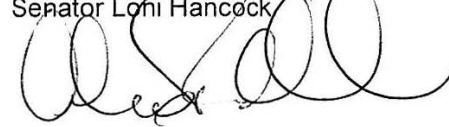
We look forward to your response on this important issue.

Sincerely,


Senator Elaine Alquist


Senator Christine Kehoe


Senator Loni Hancock


Senator Alex Padilla

/bf

Attachment

Appendix 6: An Analysis of Barriers to Implementing Airport-Style Security at all Points of Entry to California's Correctional Institutions, January 2012

AN ANALYSIS OF BARRIERS TO IMPLEMENTING AIRPORT-STYLE SECURITY AT ALL POINTS OF ENTRY TO CALIFORNIA'S CORRECTIONAL INSTITUTIONS

California Department of Corrections and Rehabilitation
January 20, 2012

On October 6, 2011 Governor Brown signed Executive Order B-11-11 addressing the public safety threat posed by contraband cellular telephones in California's prisons. The Executive Order sets forth several important findings. An increasing number of contraband telephones are being found inside our prisons. Inmates in possession of such phones often use them to commit crimes and further victimize the public, sometimes in furtherance of gang activities.

The California Department of Corrections and Rehabilitation (the Department) is committed to an aggressive, multi-pronged approach to eradicate the public safety threat posed by contraband cell phones within its correctional facilities. The Executive Order requires that the Department continue these efforts, including more thorough searches of people who enter prisons; an increased number of random searches of inmates' cells, prison property, and employees; increased penalties for inmates in possession of contraband devices and anyone who illegally provides contraband devices to inmates; and an increased use of canines and state-of-the-art technology to find and confiscate contraband cellular devices. The Executive Order also requires the Department to "develop and deploy a cost-efficient system to interrupt unauthorized cellular transmissions at California's prisons in a manner consistent with federal law." The Department is already zealously pursuing each of these efforts.

The Executive Order also discusses the challenges associated with preventing contraband cellular telephones from entering the prisons in the first place. In particular, the Executive Order explains that the Department "lacks airport-style security screening for people who enter prisons." Moreover, instituting such measures "could be costly at a time when the state is facing severe budget restrictions" given that California has "one of the largest prison systems in the world, and there are hundreds of entry points through which these devices can be smuggled." To better assess these challenges, the Executive Order requires the Department to "immediately review and prepare an analysis of any barriers to implementing airport-style security screening at all points of entry to California's correctional institutions." This report sets forth that analysis.

In order to fulfill the Executive Order's mandate to determine the feasibility of implementing airport-style security screening, it is necessary to first define what airport-style security screening means. To answer that question, the Department reviewed the feasibility of implementing a multi-layered screening approach similar to those found in major airports across the country. These security methods include criminal sanctions for the unauthorized possession of contraband items; random searches, including "pat downs"; use of specially trained canines; use of hand-held metal detection devices; video surveillance; limits to personal belongings; and increased use of metal detectors or body scanning equipment to search property and persons. Accordingly, we use "airport-style security screening" to refer to a multi-layered approach that combines all of these components.

We now turn our attention to each component of airport-style security. For each element, we note whether it has in fact already been implemented. If not, we provide a discussion of any barriers to implementation.

I. Criminal Penalties for Unauthorized Cellular Telephone Possession

An essential element of airport-style security screening must be legislation that assesses serious penalties for the unauthorized possession of contraband items. Indeed, it would make little sense to invest in robust airport-style security screening without the presence of a sufficient disincentive for violating the security strictures. Without an appropriate statutory sanction, any investment in airport-style security screening is squandered.

Notably, California lacked this bedrock element until recently. On October 5, 2011, the Governor signed Senate Bill 26 (Padilla) finally establishing for the first time in California a criminal disincentive for visitors and staff to provide cellular telephones to inmates. The new law makes it a misdemeanor for a person to possess a cellular telephone with the intent of delivering it to an inmate. The bill also creates administrative penalties – credit loss – for inmates found in possession of cellular telephones. This landmark legislation establishes the requisite foundation for any robust system of prison security.

California has enacted legislation that establishes criminal penalties for the unauthorized possession of cellular telephones and the Department is now enforcing this law throughout our prison system. Accordingly, this foundational element of airport-style security screening is implemented.

II. Random Searches and Pat-Downs of Staff Entering Prisons

Random searches, including pat-downs, are a fundamental and effective component of any system of airport-style security. These searches comprise visual, and sometimes physical, inspections of staff and their belongings.

In 2009 the Department stepped up its efforts to stop cellular telephones from being transported inside of our prisons by launching *Operation Disconnect*, an aggressive effort to increase the number and quality of random staff searches. As part of *Operation Disconnect*, staff are subject to regular surprise searches. Several times each month at all prisons, facility access points are confidentially identified where staff are then stopped and subjected to review for possession of contraband. Staff must empty their pockets, remove their jackets and open their lunch boxes and briefcases. In 2011, 463 *Operation Disconnect* searches were conducted and 169 cell phones confiscated. Employees who transmit cell phones to inmates are terminated from state service.

Operation Disconnect represents a low-cost solution by allowing the use of existing staff to be intermittently redirected for random searches of staff. Additionally, given that such random searches are conducted at infrequent intervals, the processing of staff is not as time-consuming as would be the case if CDCR were to conduct searches upon all staff entering the prison.

Under *Operation Disconnect*, the Department has established an effective system of random searches, including pat-downs. As a result, this component of airport-style security has been implemented.

III. Canine Detection

As a familiar presence in airports, canines are a well-known aspect of airport-style security. Less known is the role that canines can play in terms of cellular telephone detection. Indeed, the last several years have seen a nationwide expansion among state prison systems in the use of canines for contraband detection. The dogs can be specifically trained to find cellular telephones through their sense of smell.

California began implementing the use of canine detection several years ago and now has the largest cellular telephone-sniffing canine unit in the nation. The Department has 30 dogs statewide (some dogs are trained to detect cell phones and others are trained to detect drugs) at almost no cost to the state. Nearly all of the dogs have been donated or rescued. Staff positions associated with handling the dogs have been mostly absorbed within existing duties. At its present level of deployment, this is a low-cost and effective tool in cell phone interdiction. Since May 2009, these canines have resulted in location of 1,909 cellular telephones as well as assorted components such as power cords, SIM cards, and batteries.

Canine detection is presently limited to searches of prison cells and common areas in inmate housing. Searching visitors using canines is more problematic. The Department's efforts to use canines to search visitor vehicles for contraband has been suspended since 1986, when the court issued the permanent injunction in the case of *Estes v. Rowland*.¹ The permanent injunction requires that any policies and procedures governing these searches be codified in regulations prior to the resumption of the canine search program, something that to date has not occurred. While the *Estes* injunction mainly addresses the use of dogs to search visitors' vehicles and not their persons, the injunction requires that dogs be kept at least twenty feet away from visitors. Due to the scent-based nature of the search for cell phones, this minimum distance requirement renders canine searches of visitors useless.

The Department would welcome the further expansion of canine detection, but any further expansion would require additional resources as existing resources have already been maximized. At full deployment, the Department could utilize an additional 15 dogs and at least one additional sworn position associated with each dog. Additional resources for housing the dogs may also be necessary.

Even without any further expansion, the Department has an effective canine detection unit as part of its interdiction strategy. Accordingly, this aspect of airport-style security should be considered implemented.

¹ *Estes v. Rowland* (Judgment issued December 4, 1989, No.127247) as modified by *Estes v. Rowland* (1993) 14 Cal.App.4th 508.

IV. Metal-Detection Wands

Some airport-style security systems utilize hand-held metal detectors commonly referred to as wands. The Department currently has hundreds of hand-held metal detection devices within its prisons. Relatively inexpensive (approximately \$110 per wand), they are routinely used for large-scale inmate movements and less frequently used in searches of visitors. They are not currently used on staff, in part because the large number of metal objects that staff are required to carry would be triggered by a wand, ultimately resulting in the time-consuming divestiture of equipment and gear. The Department would be required to compensate staff for this time, a considerable expense given the frequent comings and goings of staff throughout the workday.

Unfortunately, wands are not always effective in picking up objects with lower amounts of metal materials. With cell phones increasingly made of smaller amounts of metals, the Department has explored more sophisticated technologies that will alert to smaller amounts of metal. In 2011 the Department piloted equipment that can be carried and placed throughout a facility as needed, such as when a line of persons forms or as deliveries are received. The technology was a ferrous metal detector and can alert on minute quantities of metals. In addition to this flexibility, its radius technology can also detect phones secreted in shoes, a common smuggling tactic and a weakness of most standing metal detectors that can seldom detect metals at floor level. The Department is currently analyzing the results of this study and will continue to explore the effectiveness and feasibility of ferrous metal detection. Each ferrous metal detection device costs approximately \$9,000.



Ferrous metal detector

The Department currently uses metal-detection wands for searches of inmates and staff. This element of airport-style security is therefore implemented. Further investment in this strategy, such as the purchase of ferrous metal detection devices for each of the Department's 33 prisons, would require additional resources as described above.

V. Video Surveillance

The Department has added video surveillance to its facilities over the years to both monitor and record events in the prison. Video surveillance thus serves a number of purposes beyond simply contraband interdiction.

While video cameras may be of use in preventing unauthorized cell phones from coming into correctional facilities, their value in this area is limited. Should perpetrators of a crime learn where cameras are located, they either avoid committing crimes in those areas or shield their identities. Video surveillance is also limited by its physical scope and resolution: it can only successfully capture a small portion of what occurs within its purview. In this way, video cameras cannot take the place of active personnel surveillance in the areas being monitored.

Video surveillance obviously carries costs. Video camera equipment costs approximately \$12,375. There are also staffing costs associated with reviewing video recordings.

In light of these limitations, the Department will continue its modest investment in video surveillance, in part for reasons beyond cellular telephone interdiction. This element of airport-style security should be considered implemented. Insofar as further expansion of this tool is sought, the Department would incur the additional costs set forth above.

VI. Limitations on Personal Property That May be Brought into a Facility

The Department has explored whether interdiction efforts could be supported through the required use of clear plastic containers for all personal belongings. Proponents suggest that this would also speed up searches of personal property by eliminating the need to unpack certain bags and lunchboxes.

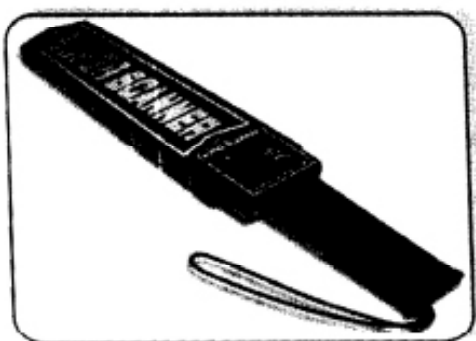
Unfortunately, our own experience is that the smuggling of contraband cellular telephones can easily adapt to evade this technology. The adoption of clear plastic requirements would leave personal clothing, and likely purses and handbags, unaffected. Contraband items can be easily secreted in these areas. This solution, which nonetheless may merit further exploration, appears now to present little value in the fight against contraband cellular telephones.

VII. Metal Detectors and Body Scanning Technology

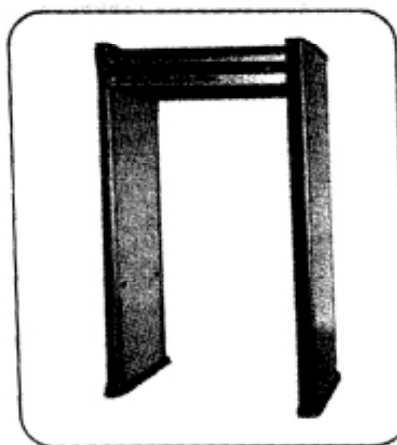
The primary component of airport-style security screening is the use of metal detectors, x-ray machines, body scanning technology, or some combination thereof, at all points of entry into California's prisons. This component represents one of the most effective strategies in cellular telephone interdiction. Unfortunately, it is also the aspect of airport-style security screening that California lacks.

The Department does have over 250 older-style standing metal detectors used primarily in visitor and inmate processing areas. However, these types of older metal detectors often cannot detect cellular telephones if they are secreted in the body cavity, especially if the battery is removed. Moreover, all metal detectors fail to reliably detect SIM cards. And while the interdiction of other contraband items beyond cellular telephones is not the subject of this analysis, obviously the Department would prefer to adopt a technological solution that also serves interdiction efforts in regards to other, non-metal contraband such as tobacco, drugs and unauthorized communications. Metal detectors cannot assist in the interdiction of any of these items.

Hand-Held Wand Metal Detection Device



Standing Metal Detector



Beyond its limited effectiveness, metal detection would also be a particularly expensive technology to pursue. First of all, the devices themselves range from \$3,000 to \$9,000. Each of California's 33 adult prisons would need at least one, and those facilities with more than one point of entry would need more.

The use of metal detectors also comes with a high cost for the time delays caused by the screening. Many departmental employees arrive for work in full uniform, with several metal-containing items and other objects that would trigger a metal detection device. The removal,

search, retrieval, and donning of removed items would result in significant delays for every employee. It is also worth bearing in mind that staff may enter and leave through the secure screening area several times per day, thereby multiplying these costs.

During each day's three shift changes the delays could be particularly acute as employees are forced to wait in line for this process – a tremendous fiscal burden that the Department may be required to absorb. The Department is currently litigating *California Correctional Employees Wage and Hour Cases*, also known as the "Stoezl class action," a coordinated proceeding involving three separate cases.² These cases involve certified class action allegations by individuals³ alleging that they have not been fully compensated for pre- and post- shift work activities. Plaintiffs allege that the stations where they are required to sign in and out are often significantly removed from their actual work posts. In order to ensure that they are at their posts at their assigned start and stop times, they claim they must sign in early and sign out late, due to the time it takes to travel within an institution between the place of entry to the facility and the work posts. Should plaintiffs prevail, the costs of screening all employees at the gates would rise by whatever additional time the screening adds to the pre-shift time period.

New body scanning technology overcomes some of the limitations and delay-associated costs that plague metal detectors by permitting a single, all-inclusive view of both personal property, whether metallic or not, and the body, thereby negating the need for divestiture and its concomitant delays. As technology has improved to allow greater image clarity, as well as lowered radiation emissions now within OSHA standards, airports have begun using body scanning equipment to screen passengers, rather than metal detectors.

Initially, airports used x-ray equipment, which relied on radiation transmission. More recently, however, airports have begun to use millimeter wave equipment, a more effective screening system that avoids the use of radiation.

Each method has its drawbacks. Radiation concerns associated with x-ray equipment have led to a lawsuit against the federal government. In California, a similar claim in *Harrington-Wisely v. State of California* has resulted in an injunction barring the Department from use of its x-ray equipment to conduct searches of prison visitors. That injunction expires in March 2013. Millimeter wave equipment, on the other hand, has its critics who claim that the procedure, which yields a detailed image of the subject's body, violates privacy.

² *Stoezl, Kurt, et al v. CDCR, et al.* San Francisco County Superior Court Case No. CGC-08-474096; *Shaw, Jaime, et al. v. CDCR, et al.* Kings County Superior Court Case No.: 10 C0081; and *Kuhn, Stanley, et al. v. CDCR, et al.* Los Angeles County Superior Court Case No.: BC450446.

³ The class size has been estimated to be approximately 40,000 individuals, which consist of all persons who are or who have been employed as Correctional Officers, Correctional Sergeants, Correctional Lieutenants, Medical Technical Assistants, Senior Medical Technical Assistants, Correctional Counselors I, Correctional Counselors II, Youth Correctional Officers, and/or Youth Correctional Counselors to work at adult and/or youth correctional institutions within the California Department of Corrections and Rehabilitation (CDCR) and Department of Mental Health (DMH) institutions in the period commencing April 9, 2005 until the notice of pendency of the class action.

Appendix 7: Federal Bureau of Prisons Electronic Search Protocol²⁹

1. All staff will be required to clear a metal detection device prior to gaining access to the secure confines of the institution. "Secure confines" for this purpose generally means entering the secured inner perimeter of the institution.

Electronic searches of all Bureau of Prisons staff will be conducted via walk-through or hand-held metal detectors by designated staff member(s). No inmate visitors will be allowed to remain in the area, or allowed to view screening procedures, when electronic searches of staff are being conducted.

It is the responsibility of the employee to clear the metal detector by either passing all items through the metal detector or by placing all items on an available x-ray machine for screening. If the staff member is unable to determine the origin of the item causing the metal detector activation, a designated supervisor will be consulted immediately to determine the next appropriate step to clear or deny the employee for entry. An adequate private screening area for staff will be made available for this purpose. Employees will be allowed to take any items not able to clear the metal detector or x-ray machine to their vehicles, unless doing so would jeopardize the safety, security, or good order to the institution. Existing limited secure storage for cell phones and other personal items (not otherwise prohibited) will be provided for staff that commute via public transportation.

Employees leaving the secure confines of the institution during their shifts are required to clear metal detection upon re-entering the institution.

2. During the initial six weeks of implementation of these procedures, management agrees to meet weekly, or at a mutually agreed upon time, with the Union President or designee to review institution policies and procedural changes due to the implementation of electronic searches.
3. Employees required to perform work in excess of their regularly scheduled hours will be compensated in accordance with applicable laws, rules, and regulations.
4. Employees with a non-paid duty-free lunch break will be afforded their full 30 minutes lunch break. Employees who leave the institution for lunch will be allowed a reasonable amount of time to return to their post in the event of unusual and unforeseen delays in clearing the metal detection screening process.
5. During the initial six weeks of the implementation of electronic searches, a supervisor (excluding an employee serving in an acting capacity) or management official will be in the search area assisting with screening.
6. After the initial six weeks, management will ensure a second staff member is available to expedite the screening process during peak hours. A designated supervisor or management official will be available via radio or telephone for consultation on any issue that may occur. After the initial six-week observation period, staff will contact a designated supervisor to address any concerns that may arise. Each Chief Executive Officer (CEO) will define peak periods for staff entering their institution either by issuing a memorandum to all staff, or posting the information by a method available to all staff, such as an electronic message board in the front lobby.
7. A radiation exposure badge will be in the immediate search area of each x-ray machine. Periodically these badges will be evaluated for exposure levels.
8. Staff required to utilize the x-ray/metal detectors will receive appropriate training prior to

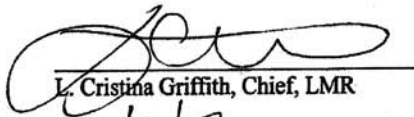
²⁹ Source: Federal Bureau of Prisons

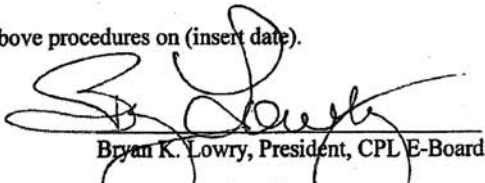
- being assigned to any post requiring the operation of these devices.
9. Staff members who have medical conditions that will not allow them to clear or pass through electronic screening devices will be issued a pass by the Warden, upon receipt of administratively acceptable medical documentation (e.g., medical certificate, a physician issued medical ID card, etc.) indicating their medical condition and the extent of the restriction(s) regarding their ability to clear electronic screening. Management agrees to abide by all appropriate privacy laws and will make adjustments to this requirement as needed.

The medical pass does not exempt the employee and their property from clearing the electronic screening but will be tailored to the employee's specific medical issues.

10. Safety-toed footwear will be in accordance with the Master Agreement. Eligible employees will have the option of an equivalent composite safety-toed footwear during their next issuance.
11. Random pat searches of staff persons, random visual searches of staff belongings, and random searches of staff vehicles are not permitted pursuant to these procedures.
12. Staff remain subject to the same reasonable suspicion searches, detention, and arrest, as provided in the Bureau policy on Searching, Detaining, or Arresting Visitors To Bureau Grounds and Facilities.

The union and management agree to the above procedures on (insert date).


L. Cristina Griffith, Chief, LMR
11/8/07
Date


Bryan K. Lowry, President, CPL E-Board
11-8-07
Date

Appendix 8:

1. What is Radio Frequency (RF) Communications - The Idea of Waves as Energy

This section provides an overview of the physics of moving information or intelligence via a radio wave generated by an electronic circuit.

What is a Radio Wave?

The best analogy is the waves that move across the surface of water. These waves are identical to radio waves in the basic physics of motion as a result of some type of stimulus. Waves on water are caused by a disturbance of the surface of the water. These waves are created when the surface of the water is perturbed in some way, for example a rock is dropped into the water. As the rock passes through the surface the stimulus of this passing pushes water out its path. This pushing action creates waves that emanate outwards from the point of entry. The size of wave is directly proportional to the weight of the rock and the spacing between the waves is directly proportional to the speed of the rock. The speed and weight of the rock are directly coupled physically so the waves move outward carrying both the frequency and power this physical transfer of energy created. These waves move in perfect symmetry in all directions simultaneously, until an obstacle is encountered. When a portion of the wave encounters an obstacle the wave shape, size and speed are changed. Now there are multiple waves traveling across the water's surface, each correlated to the others in that they came from the same source, but different because some of the wave has been disturbed. Radio waves do the same thing in air.

The relationship between these slow moving physical waves in the water and high-speed invisible radio waves is in the use of the terms "power" and "frequency". The power of the wave is how high it is above the non-disturbed water's surface, and the frequency is how many waves pass the same point in one second. In radio waves the power is the "electronic force" pushing the electrons into the air and the frequency is how many times per second does a "new" wave start moving into the air.

Another thing water and radio waves have in common is the physical phenomenon of the distance they travel. Once generated, undisturbed water waves can travel extreme distances, continually getting smaller and smaller, thus losing "power" but maintaining the number of waves per second passing any point (frequency). Radio waves do the same thing. And, when water based waves encounter other water based waves at the point of intersection they interfere with each other's power and frequency. Radio waves do the same thing.

Overview of RF

Radio Frequency (RF) transmissions are emissions of radio waves that transmit information. These emissions can be transmitted and received by antennas to allow for wireless communication. Common types of RF transmissions are radio (AM/FM) signals, terrestrial television signals (over-the-air television) and wireless communications such as cellular phones, Wi-Fi (IEEE 802.11 based wireless local area networks) and Bluetooth (personal area network technology). Frequencies are identified using the measurement of Hertz (Hz). Hertz refers to the number of oscillations per second; therefore a signal at the frequency of 300Hz would oscillate 300 times every second, and a signal at the frequency of 2.4GHz would oscillate 2.4 million times every second.

RF Frequencies

Frequencies can be thought of as channels (such as television) or stations (such as radio). In fact, both TV channels and radio stations correspond directly to a frequency being used. KTXL in Sacramento, CA is channel 40. This channel assignment corresponds with the frequencies of 626-632MHz with picture, audio and other signals being broadcast at specific frequencies in that range. California State University, Sacramento (CSUS) radio station KXJZ is broadcasting at the frequency of 88.9MHz.

Many people are familiar with 2.4GHz, which is the operating frequency for many household products such as Wi-Fi and Bluetooth. Terms such as 2.4GHz are commonly used to describe a range of frequencies that are allocated to a common use. In this instance, 2.4GHz refers to the range of frequencies between 2.4GHz and 2.5GHz that are allocated for Industrial, Scientific and Measurement (ISM) purposes. The most important parameter of this band is that it is unlicensed, meaning that anybody can operate in that frequency range, which is why you can own a 2.4GHz router and operate it without an FCC license. Most bands, which are licensed, require authorization from the FCC (within the U.S.; similar agencies exist in other countries worldwide) to operate using those frequencies. Examples of commonly used licensed bands are 850MHz and 1900MHz cellular frequency bands. Shown below are the International Telecommunications Union (ITU) band allotments for RF spectrum. The Very High Frequency (VHF) frequency band is broken up to provide an example of how the frequencies within a band are utilized. In this image only a few of the selected uses are shown, many more exist within the band.

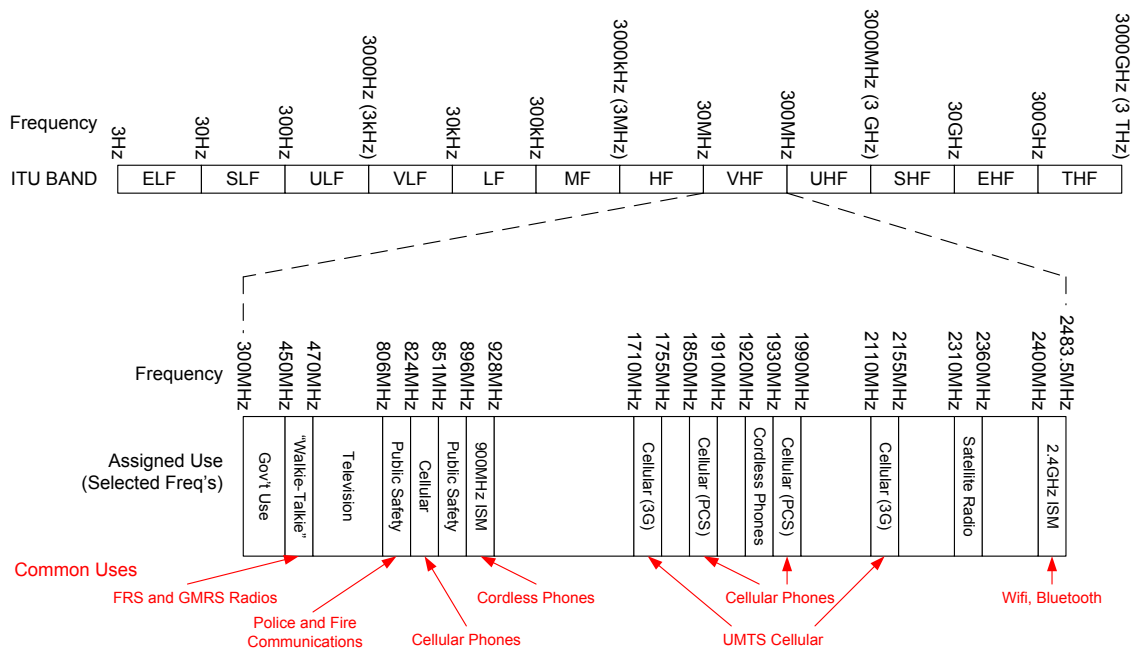


Figure 1. International Telecommunications Union (ITU) band allotments for RF spectrum.

RF Signals

To construct an RF signal, the data to be sent must be converted to a waveform, which will be transmitted via an antenna. To do this, as shown in Figure. 2, data is recorded and converted (if recorded digitally) to an analog waveform. This waveform is then modulated to the carrier frequency (88.9MHz in the case of KXJZ). This signal is amplified and transmitted via an antenna. On the receiver's end, the receiver would be tuned to the desired frequency. This tuning will allow the desired signal to be passed, with all other signals (e.g. other radio stations) blocked. The signal is then demodulated to remove the carrier and the data can then be recovered.

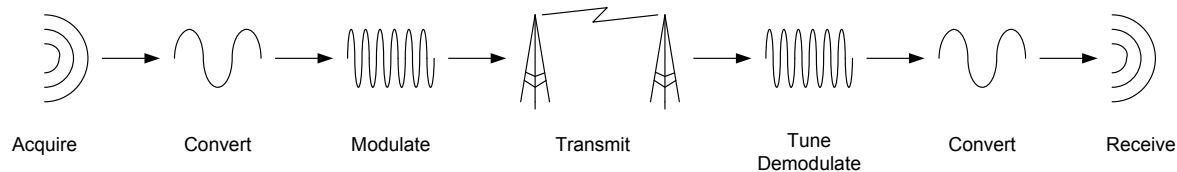


Figure 2. RF Signal Transmission

RF Transmission and Environmental Effects

Signal Propagation

Signal propagation refers to how an RF signal reacts between the transmitter and receiver due to effects of the environment. Buildings, foliage, distance and antennas all play a part in how a signal goes from point A to point B. The ability to receive a transmitted signal has to do with its signal strength at the receiver. The signal strength is affected by the transmitted power level (generally, the higher the transmitted power, the higher the received power), obstacles such as trees and buildings (generally, the fewer obstacles, the higher the received power) and antenna height (generally, the higher the antennas, the higher the received power).

Cellular dead spots, FM Radio static and poor Wi-Fi reception are just some of the examples of negative effects on signal propagation that people experience on a daily basis.

Signal Multipath

Signal multipath refers to the signal effects when it bounces around, either due to external objects such as land (e.g. mountains) or buildings. Multipath can be noticed by a receiver as a copy of the original signal, similar to an echo.

Signal Interference

Signal interference occurs when another signal is transmitting at the same or a similar frequency. This can be due to the fact that signals aren't strict in their frequencies and will "bleed" to adjacent frequency bands, or do to multiple signals at the same frequency, particularly in unlicensed operations, such as Wi-Fi. When multiple signals are received at the same frequency, the receiver must differentiate the two. This can be performed using very advanced methods such as code division, where each signal is encoded with a specific code, or very simple methods such as power levels, where the strongest signal is used.

In a perfect world, transmission would be limited to the desired bands and on a plot of frequency, would look like a rectangle. Unfortunately, due to the real world effects on RF signals, signals tend to look like figure 3 below, with power at the frequencies trailing off as you get further and further from the desired frequency. This effect is called roll-off. This creates areas of overlap and therefore, interference, as one signal is intruding on the space reserved for another.

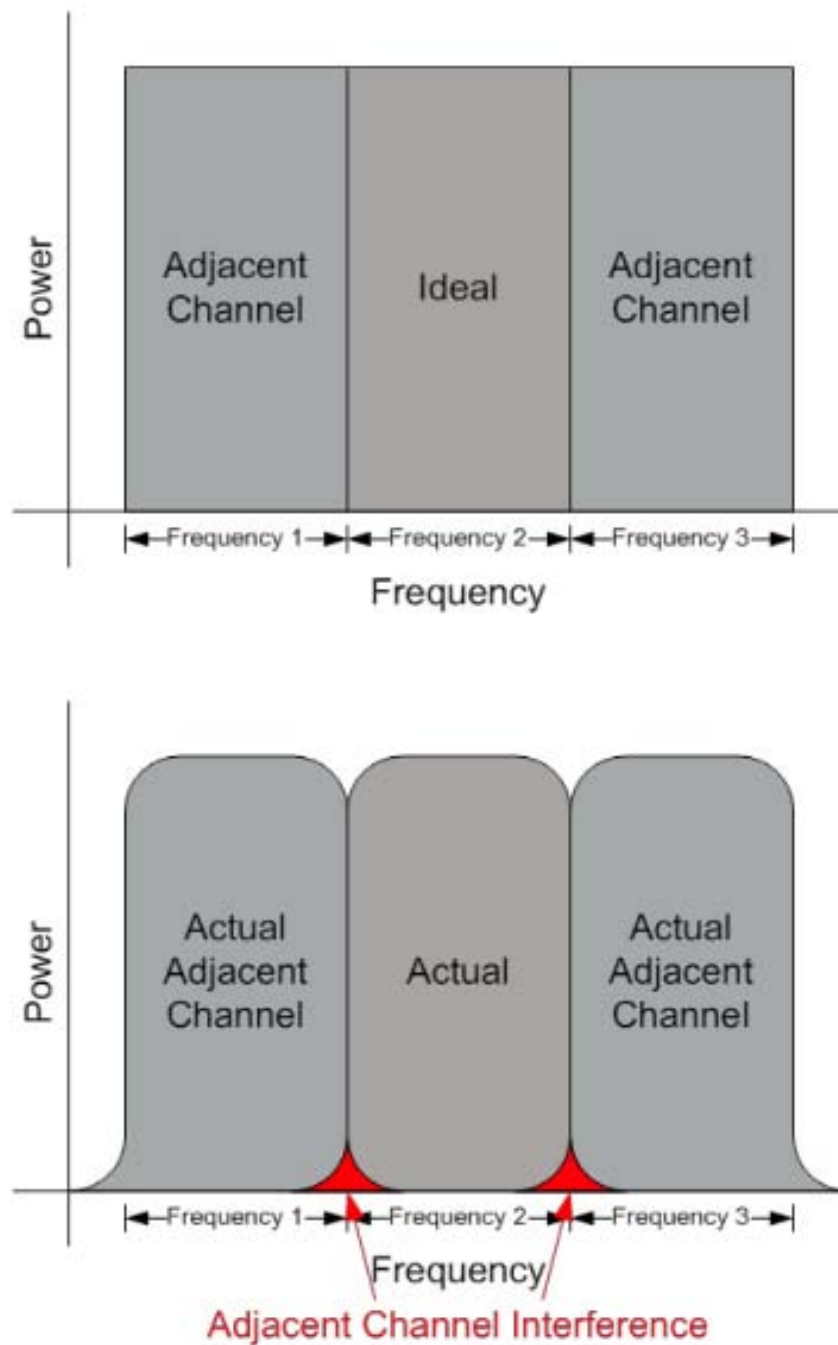


Figure 3. Real-world Transmission Problems

Guard bands are implemented to help alleviate this problem. Guard bands are frequency allotments that nobody can transmit in. But they only help so much. In many cases, interference from signals exceeds these guard bands and still overlaps into the adjacent frequency.

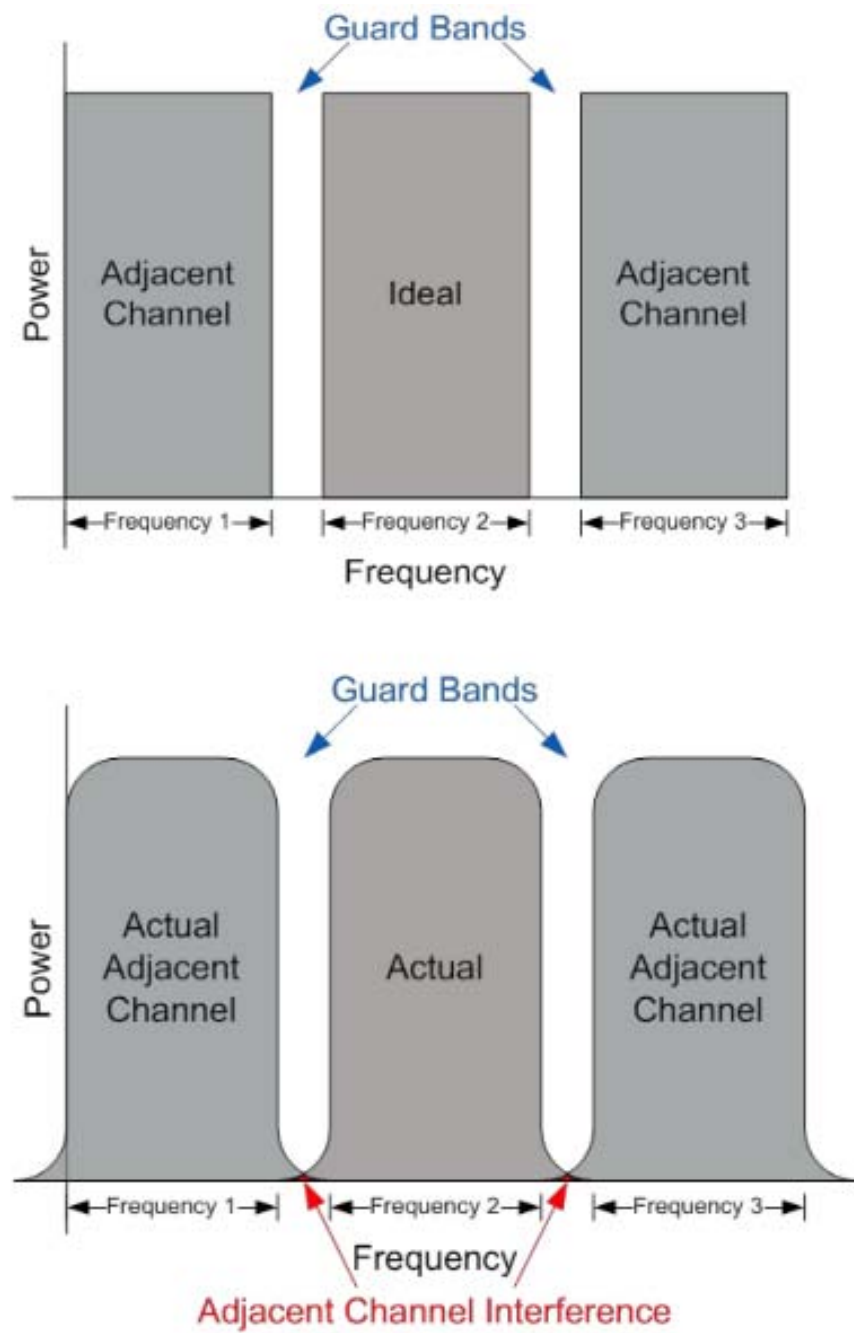


Figure 4. Guard Bands

Summary

In summary, an RF signal is energy transmitted at a certain frequency, which is effected by many outside influences. In many ways, RF is very similar to holding a discussion at a loud cocktail party. Many of the functions have an analogous equivalent, as shown in the table below.

Function	RF	Cocktail Party Equivalent
Signal Acquisition	Acquire Data	Speaker makes sound
Signal Conversion	Format Data	Speaker uses words
Signal Modulation	Data modulated to carrier freq.	Speaker's voice
Signal Transmission	Carrier freq. transmitted	Speaker speaks
Signal Propagation	Path loss due to distance, environment, etc.	Difficulty hearing due to distance
Signal Multipath		Difficulty hearing due to echo, reverb
Signal Interference	Other signals at the same, or close frequencies	Other speakers in the room
Signal Tuning/ Demodulation	Only the desired frequencies are passed, undesired frequencies are blocked	Singling out the desired speakers voice
Signal Conversion	Reading the data in the proper format	Understanding the speakers words and language
Signal Reception	Playing data	Listening to the speaker

Table 1. Cocktail Party Comparisons

2. Communications Technologies

Mobile Phone Technology

There are many types of mobile communications technologies. The most common are cell phones. Cell phones can be characterized by their radio access technologies, such as CDMA, GSM, iDEN, WCDMA and LTE. These technologies determine the way in which data is transmitted between the cell phone and the cell tower.

Multiple carriers provide service utilizing various access technologies in the state of California. Licensed network operators in California, and their radio access technologies are shown in the table below.

Operator	Radio Access Technologies
AT&T Wireless	GSM, GPRS, EDGE, UMTS/HSPA, LTE
Cricket	CDMA, CDMA2000, EV-DO
Metro PCS	CDMA2000, EV-DO, LTE
Sprint PCS	CDMA2000, EV-DO, iDEN
T-Mobile	GSM, GPRS, EDGE, UMTS
Verizon Wireless	CDMA, CDMA2000, EV-DO, LTE

Table 2. Network Operators in California

Mobile Phone Standards

Three families of cellular standards exist, and each is overseen by a standards organization. These organizations are known as the 3rd Generation Partnership Project (3GPP), which sets the standards for GSM based systems; 3rd Generation Partnership Project 2 (3GPP2), which sets the standards for CDMA based systems; and the Institute of Electrical and Electronics Engineers (IEEE), which sets the standards for WiMax based systems. The standards bodies have developed wireless communication network protocols that are categorized by generation, and referred to as 1G, 2G, 3G and 4G.

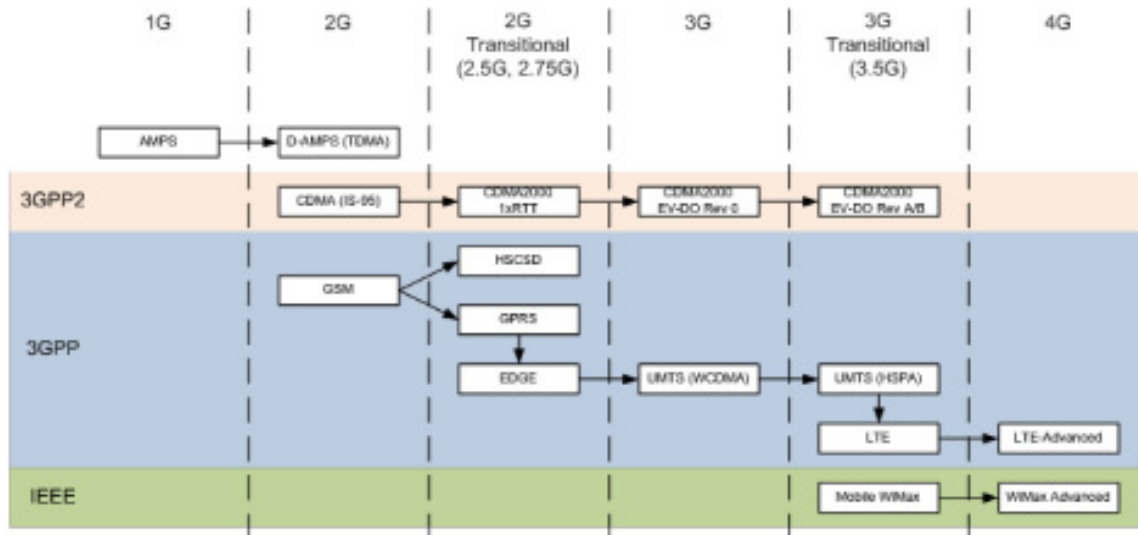


Figure 5. Defining Generations of Networks

First generation (1G) networks (e.g. Analog AMPS) were analog, voice-only, circuit switched networks, creating a wireless parallel to the common wire line telecommunications infrastructure. Second generation (2G) networks (e.g. GSM, CDMA) advanced the existing networks by upgrading to digital technologies that provided a more efficient use of resources. Enhancements were made to 2G networks to add a packet-switched data overlay to the existing networks. These enhancements were referred to as both 2.5G and 2.75G (e.g. GPRS, EDGE, CDMA2000 1xRTT). Third generation (3G) networks (e.g. CDMA2000 EV-DO Rev 0, UMTS) were required to meet a new international standard, IMT-2000, which placed requirements on data transfer, most noticeably a transfer speed in excess of 200kbts/second. The networks were enhanced with an all-IP based overlay, commonly referred to as 3.5G (e.g. CDMA2000 EV-DO Rev. A, UMTS/HSPA). The newest generation, fourth generation (4G) networks (e.g. LTE Advanced and WiMax Advanced), is currently being deployed as all-Internet Protocol (IP) networks. These networks treat all traffic (including voice) as data, so voice is provided through Voice-over-IP (VoIP) protocols. These networks are required to meet the IMT-Advanced standard, which places additional requirements on data transfer, notably transfer speeds in excess of 100Mbps/second for mobile users and 1Gbit/second for stationary users. The following table summarizes the common network protocols by generation and standards body.

Generation	Family	Voice Protocol	Data Protocol(s)
1G		AMPS	N/A
2G	3GPP	GSM	Circuit-Switched Data
	3GPP2	CDMA	Circuit-Switched Data
2G+	3GPP	GSM	GPRS (2.5G), EDGE (2.75G)
	3GPP2	CDMA2000	CDMA2000 1xRTT
3G	3GPP	GSM	UMTS, WCDMA
	3GPP2	CDMA2000	CDMA2000 1xEV-DO
3G+	3GPP	GSM	HSPA, LTE
	3GPP2	CDMA2000	CDMA2000 1xEV-DO Rev A
	IEEE	N/A	Mobile WiMax
4G	3GPP	N/A	LTE-Advanced
	IEEE	N/A	WiMax-Advanced

Table 3. Common Network Protocols by Generation and Standards Body

Regardless of the technology implemented, all mobile communication systems rely on a network of terrestrial cellular towers with antennas to provide coverage to a given geographic area. Cell towers are typically located in a manner to prevent them from interfering with each other. The telephone carriers are allocated FCC licensed frequencies, so that extraneous interference should be minimized. The selection of a particular tower a cell phone will connect to at any one time depends on many variables such as signal strength. A cell phone will attempt to connect with a rogue device emulating a tower if it meets the necessary criteria and operates on the appropriate frequencies.

Network Identities

CDMA devices use an electronic serial number, known as the Mobile Equipment Identifier (MEID) embedded in their devices, while GSM devices utilize the IMEI (International Mobile Equipment Identifier) to identify the phone equipment and the IMSI (International Mobile Subscriber Identifier), which resides on the SIM (Subscriber Identity Module), card to identify the user.

Frequency Use

Networks operate on a variety of licensed frequency bands and a specific network's frequency may change based on geographic area. In the U.S., the cellular frequency bands used are the 850MHz and 1900MHz bands for 2G, 3G and 4G networks; as well as 700MHz and 2100MHz for newer 3G and 4G networks. Foreign countries permit cell phones to operate in different frequency ranges. Worldwide, the most common frequency bands are 450MHz, 900MHz and 1800MHz.

Locating a Cellular Phone

Locating a cellular phone can be done in multiple ways. From the network side, it is possible to identify which cellular towers are in close proximity to a specific cell phone. Typically, a cellular phone can "see" as many as six cellular towers at any given point in time. Given the (up to) six towers in range, and approximate RF power levels, a crude determination of location (to within 10s or 100s of meters) can be calculated. Most modern cellular phones have GPS capabilities (due to e911 requirements) that allow for the network to obtain the GPS location of the cellular phone.

Without network intervention, the presence and approximate location of a cellular phone (without identifying the device) can be determined by looking for traffic in the cellular uplink frequency channels. These uplink frequency channels are the range of frequencies used by cellular phones to communicate to cellular towers. Downlink channels are the corresponding frequencies that the cellular towers use to communicate with a cellular phone. Monitoring these frequencies will only alert you to the presence of a cellular tower.

While locating a cellular phone using the uplink frequency channel isn't extremely accurate, relative power levels will provide an indication of proximity to the cellular phone. Just as a human can listen to locate the source of a sound, an RF spectrum analyzer can listen to the RF emissions to locate the source, in this case a cellular phone. Just as the volume gets louder as the listener nears the source of the sound, the RF emissions get more powerful as the receiver nears the source of the emission, in this case, the cellular phone. This is the basic premise for most cellular detection devices.

One drawback to locating a cellular phone this way is that it does require the phone to be powered on. Phones do not emit RF energy when powered off and therefore cannot be located with this technique. In addition, the output power level of the phone varies depending on the activity of the phone (see Figure 6) and is directly correlated to the ability to detect the RF emission. As such it is much easier to detect the presence of a cellular phone when in an active voice session, and much harder to detect when idle.

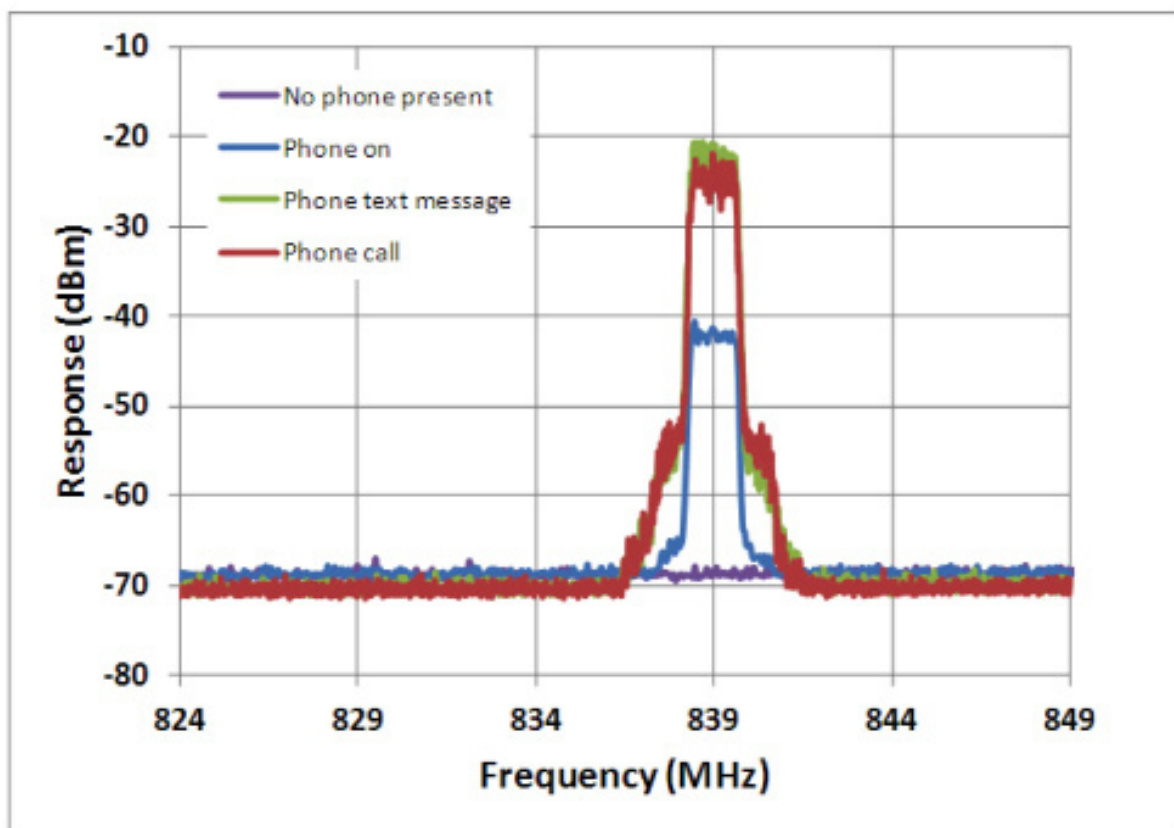


Figure 6. Power level of the phone varies depending on the activity of the phone

Wi-Fi (WLAN) Technology

Wi-Fi is probably the most ubiquitous wireless network technology. It is based on the IEEE 802.11 standards. Specifically, 802.11a, 802.11b, 802.11g, 802.11n and 802.11p provide the specifications for wireless Ethernet systems. With the maturity of Voice over Internet Protocol (VoIP) technology, Wi-Fi networks are increasingly being used for voice communications and can be accessed via many cellular phones. Wi-Fi networks operate in unlicensed frequency ranges, the most common of which reside in the 2.4GHz and 5GHz bands. However the IEEE 802.11 working group is studying the use of 60GHz band systems. Current MAS implementations do not address Wi-Fi devices.

Satellite Communications Technology

Satellite phones are mobile phones that connect to a satellite rather than a terrestrial tower. The satellite transmission is in the L band range (1-2 GHz). Due to advancements in electronics, the size of the satellite phones has decreased significantly in the last 10 years. Satellite phone calls are very difficult to intercept, as they only require an unobstructed path to the orbiting satellite. Current MAS implementations do not address satellite phones.

Other (Ham Radio, Walkie-Talkie, CB, Etc.)

Point-to-Multipoint Radios

Land Mobile Radios (LMR) are typically push to talk devices (as opposed to dialing a phone number). They generally operate in a point to multipoint mode with multiple devices on a particular channel. Common examples are Citizens' Band radio and walkie-talkies. These devices can commonly be found in the HF, VHF and UHF ranges. They operate in both licensed and unlicensed frequency ranges and can operate over long distances. Because these devices broadcast the signal to all units that are on the same channel, they are very difficult to deny service. Current MAS implementations do not address point-to-multipoint radios.

Personal Area Networks (PANs)

Personal Area Networks (PANs) are low-powered communication networks intended for the transfer of data a short distance, on the order of a few meters. These networks typically operate in unlicensed frequency bands, such as the 2.4GHz ISM band. A new technology using unlicensed spectrum is ZigBee. Although originally intended for data, there are Voice over ZigBee (VoZ) devices now available. This technology is based on the IEEE 802.15 standards. VoZ, Wi-Fi systems and even a GSM base station receiver (to act as a cell tower) can all be made as DIY projects for less than \$1000. Current MAS implementations do not address personal area networks.

3. Network Operation

Mobile Phone System Operation

Mobile phones rely on a network of terrestrial base stations to operate and provide an interface to the Public Switch Telephone Network (PSTN) to complete calls to landline telephones. A legally operating network will require the licensing of spectrum as well as the deployment of cellular towers to provide coverage to a geographic area. Small cellular networks can be built, without connection to the PSTN, to provide communications over a small geographic area. For legal operation these networks require the licensing of frequency spectrum, though it is not a technical requirement to their implementation.

In order for a mobile phone to place or receive calls (or SMS messages or data services), the phone must first register with the network. Once registered, the mobile phone will remain in communication with the network providing information on state and allowing for handoffs from one cell tower to another as the mobile phone moves or due to network traffic.

Wi-Fi-Based Phone System Operation

Wi-Fi devices do not require similar infrastructure to operate as a cellular phone. Wi-Fi devices can connect via the “infrastructure” method, which utilizes a Wi-Fi access point, or via the “Peer-to-Peer” method, which allows devices to communicate directly. Because no infrastructure is required, it is much easier to set up and tear down a Wi-Fi based communications network than a cellular communications network.

Satellite Phone System Operation

Satellite phones communicate with space-based satellites which in turn communicate with terrestrial ground stations to connect to the PSTN. Because of the nature of satellite communications and the physics involved, typically a clear view of the satellite is required for a call to be placed.

These techniques have a long history in the search for contraband RF equipment, since all RF equipment, by definition, broadcasts at some frequency (or frequencies). For most transmission mediums, including cellular phones, any RF receiving equipment tuned to look at the proper frequency will be able to determine that a transmitter is operating by seeing the relative power levels at a given frequency. In the licensed cellular bands, it can be assumed that any emitter in these frequency bands is a cellular phone.

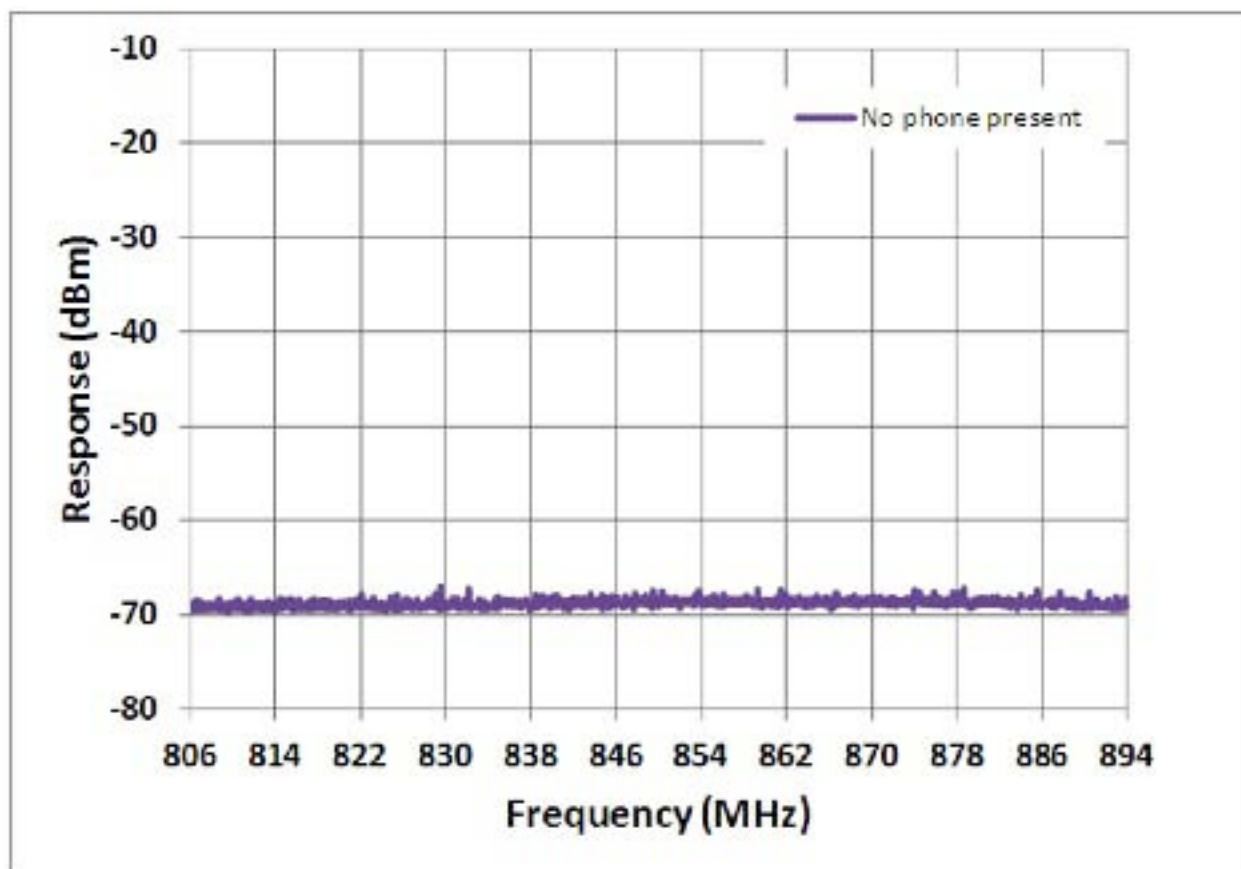


Figure 7: Noise Floor of 850MHz Cellular Band (No Transmitters Present)

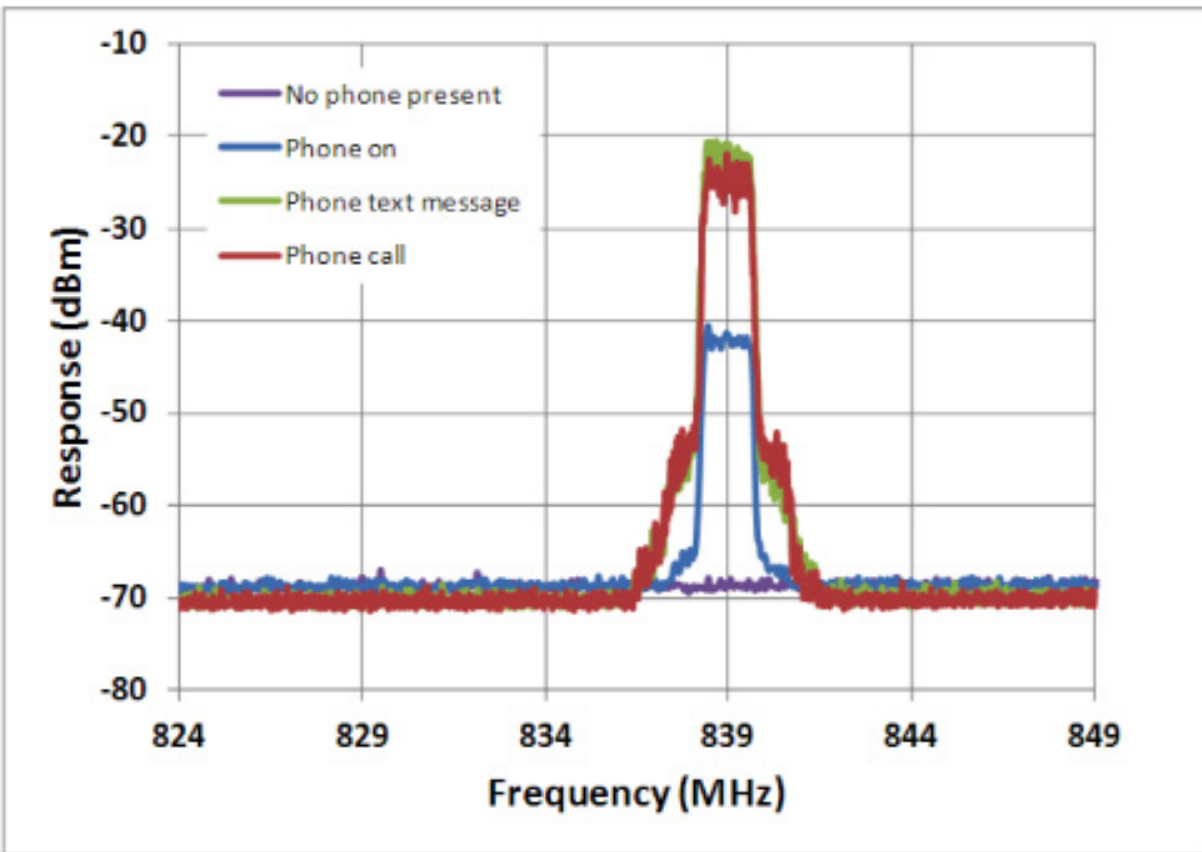


Figure 8: Power Level of Transmitting Cellular Phone

There are two standard types of detection techniques: Active and Passive. Active techniques rely on a signal output by the detection device which requests that all cellular phones in the surveillance area respond. This technique can be used to target individual devices once the IMEI or IMSI is known. Passive techniques rely on the reception of signals typically transmitted from a cellular handset to the base station (tower). In neither case is the content of the communication known.

In either technique, the relative signal strength determines the range to the handset. Absolute signal strength cannot be used because most cellular networks utilize power control in order to save battery power (cellular phones transmit at the lowest possible power level in order to close the link with the tower). When the signal from a specific cellular phone gets stronger at the detector, the detector is getting closer to the targeted cellular phone. By utilizing a direction finding (DF) technique (such as triangulation) the location of the handset can be determined.

Benefits

There are many benefits to detection techniques for locating and identifying contraband cell phones. These include ease of use, low cost, legality and covertness.

Ease of Use

Detection techniques are relatively easy to use. A portable RF receiver is tuned to the desired frequency. Once an emitter is found, the signal levels can be tracked in order to determine the location of the emitter.

Low Cost

The hardware required for detecting a cellular signal is not specialized or expensive. Systems that are able to identify devices become more expensive due to the nature of the algorithms and the additional processing required.

Legality

The use of passive cell phone detection equipment is legal and is not regulated by any FCC statute. Because active cell phone detection equipment requires transmission of signals on licensed bands, FCC regulations would restrict use of active cell phone detection equipment. Use of active equipment would require coordination with the FCC and the owners of the frequency spectrum.

Covertness

Passive cell phone detection equipment does not transmit any signal and is therefore undetectable by the cellular phone. Users of contraband cell phones will have no indication if cell phone detection equipment is deployed and currently locating their cell phone.

Active cell phone detection equipment will typically look like a cellular phone tower to which the cellular phone cannot connect. This process would occur in the background and the user would not be aware of the occurrence.

Drawbacks

Drawbacks to cell phone detection techniques include the fact that it does not interdict a cell phone call, it is manpower intensive, and it requires the device to be powered on.

Does not Interdict a Cell Phone Call

Detection techniques merely detect the presence of a powered-on cell phone. These techniques will not prevent calls or text messages from being placed.

Manpower Intensive

Since each detector needs to be mobile to effectively locate a device, it requires a commitment of manpower to operate multiple detectors. While a fixed detector arrangement could be installed into a facility, the amount of physical integration required would be high.

Requires the Cellular Device to be Powered On

The detector can only operate when a cellular phone is powered on, therefore the device must be powered on during the entire detection session. If an inmate were to power on a cellular phone for a short period of time only to receive and send a couple of text messages, or place one short duration call, it would be difficult for detection techniques to locate this user.

Comparison with Managed Access Technologies

Cell phone detection can provide the location of contraband cellular phones during some usage scenarios. Because these techniques do not prevent cellular phones from making or receiving calls, or sending or receiving text messages, this technique requires further action to prevent unwanted communications from occurring. Detection techniques have been implemented in prison facilities around the country to detect contraband cellular phones.

Examples of Detection Technologies

ITT Exelis manufactures the CellHound cellular detection system that monitors the cellular frequency bands using distributed, fixed mounted receivers that are networked together. The system has a 100-

foot range and alerts the command center when a device is present and locates the device to an area approximately the size of three prison cells.

Cellbusters manufactures the Zone Detector system, which monitors both the cellular frequency bands as well as the 2.4GHz ISM band using distributed, fixed mounted receivers that are networked together. The system has a 100-foot range and alerts the command center when a device is present and locates the device to approximately 10 feet.

BVS manufactures the Wolfhound Pro system, which monitors the cellular frequency bands using a handheld receiver. The system has a 50-foot range and alerts the operator when a device is present and locates the device to approximately 10 feet. Netline, CJAM and SecIntel also manufacture cell phone detection equipment.

Jamming Techniques

Overview

Jamming techniques utilize a wide-band RF transmitter to transmit noise at the frequencies which are to be jammed. This noise makes it hard for communications to occur at the frequencies and therefore would inhibit the use of contraband cell phones in the area of interest. Jammers can be thought of as analogous to somebody shouting loudly in close proximity. The shouting will drown out most of the normal conversations making it difficult to talk normally. When this occurs in an RF communication system, the link between the cell phone and the tower cannot be made and results in a denial of service to the user.

Benefits

There are three main benefits to the use of jamming: Ease of Use, Cost and Preventing Calls.

Ease of Use

Jammers are easy to use and set up, since they are by their very nature, a simple RF device. Transmitters are placed in areas that need to be covered and the resulting output signal provides enough noise in order to prevent communications over the frequencies in that area.

Cost

Jammers require no specialized hardware in order to operate, therefore are very inexpensive to build and maintain.

Preventing Calls

Jammers will prevent the connection between a cell phone and tower thereby preventing any communications over the cellular network. This will therefore prevent even short duration sessions from occurring.

Drawbacks

There are many potential drawbacks to jamming techniques, including interference with adjacent bands, inability to discriminate between users, difficulty in limiting the area, the overt nature of the technology, and the legality of jamming.

Interference with Adjacent Bands

It is very difficult to create jammers that affect only specific frequencies while not affecting close by frequencies. This is particularly true in the lower 800MHz bands where cellular phone frequencies are very close to public safety frequencies. It is likely that any jammer that is effective at disallowing cellular phones that use the 850MHz spectrum allotment would also

be an effective jammer of the public safety frequencies.

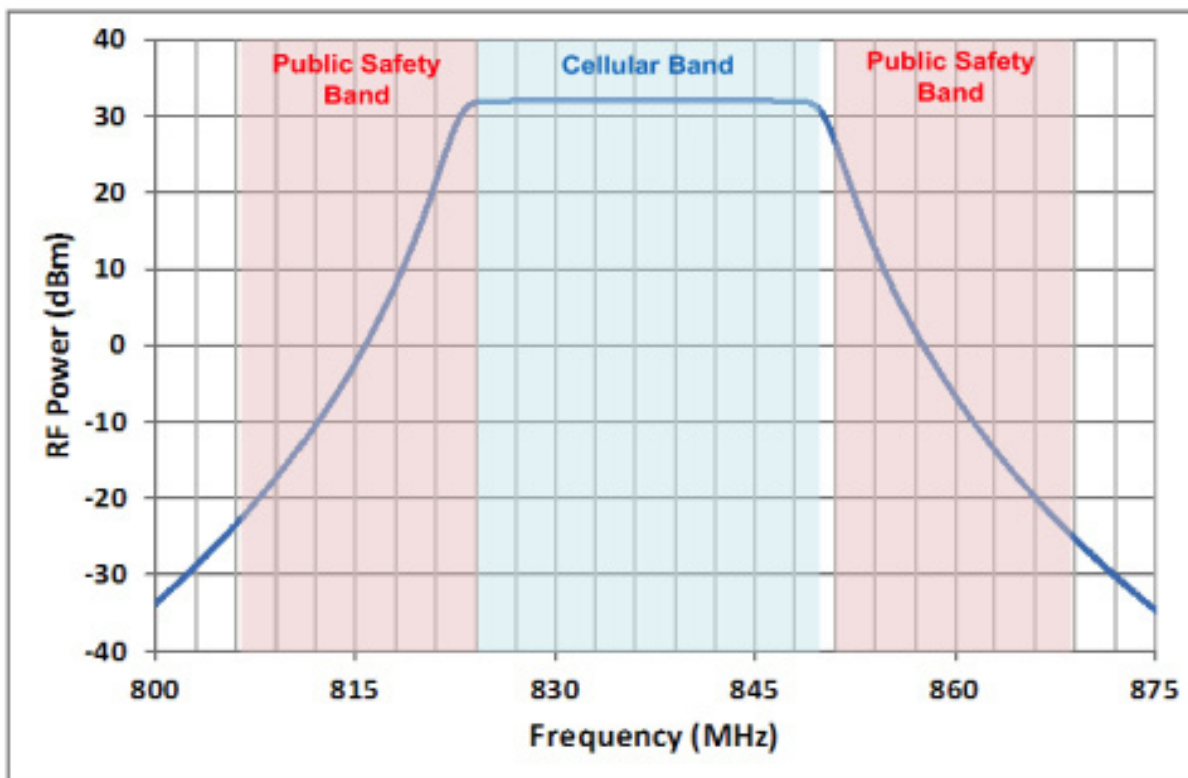


Figure 9. Public safety and cellular bands

Inability to Discriminate between Users

Jammers are a non-intelligent system, meaning that they do not have any knowledge of the users they are jamming. Therefore the lawful use of cellular devices is prevented just as well as the unlawful use. While inside the prison itself this may not be an issue, when coupled with the difficulty in limiting the affected area, this can prevent cell phones from being used near prisons as well (such as adjacent roads, etc.).

Difficulty in Limiting the Area of Coverage

Because of the nature of RF propagation, it is not possible to precisely limit the coverage area for an RF jamming signal. Due to the environment, coverage in one direction may be much greater than coverage in another. This allows for two issues to occur: unintended denial of services and jamming “deadspots”.

Unintended denial of services occurs when the jamming signal extends beyond the desired coverage area. In the case of prisons, this could mean a road adjacent to the prison, or even parts of the prisons not used by inmates, which may allow the use of cellular phones.

Jamming “deadspots” occur where the jamming signal is not strong enough due to environmental effects and will not jam a cellular signal in that area. Unlike traditional “deadspots”, jamming “deadspots” mean that the jamming signal isn’t received, but the towers signal may still be received, resulting in pockets of coverage (instead of pockets of no coverage). Over time, these locations may become known to the prison population, and the use of cell phones will migrate to these physical locations.

Overt

A jamming signal is overt. It can be easily detected and is apparent to the user when they no longer have service where service was once present. This may or may not be an issue in the prison scenario.

Legality

Jammers are illegal to operate in the United States. The FCC forbids the use of jamming equipment in licensed bands (including cellular) without an FCC waiver. However South Carolina prison officials received FCC approval to test jamming technology that intercepts and terminates cell phone calls. South Carolina officials reported that the technology was very effective at jamming cell signals without interfering with cell signals in areas adjacent to the facility. However, the approval to test was for a limited time and the FCC has not granted approval to implement the use of jamming technology.³⁰

Comparison with Managed Access Technologies

Jammers can provide many of the same benefits of managed access systems (mainly denial of service) at a much lower cost. But there are drawbacks to the technique including the inability to discriminate users, unintended denial of service and legal right to operate the jammers in licensed bands. Netline, CJam, and SecIntel all manufacture cellular jammers.

Security Screening Techniques at Points of Ingress and Egress

Overview

Standard inspection techniques, such as metal detectors and x-rays can be used to identify mobile phones at entry points. These techniques focus on detecting the devices, or parts of the device, and would require physically removing the device after detection. Metal detectors and x-rays are commonly used to search for contraband devices in prisons, airports and other secure facilities. New York has trained dogs to detect certain components found in cell phones and has implemented their use at Riker's Island.

Benefits

Security screening techniques are well understood due to their common use. Rather than identifying a device only when in use, as many of the RF based systems do, this technique identifies devices that are not operating, as well as operating.

Drawbacks

A thorough security screening can be manpower intensive and does not target contraband cellular phones specifically.

30 Special Report- "Inmate Cell Phone Use and Endangers Prison Security and Public Safety", Office of the Inspector General, David R. Shaw, Inspector General, State of California, May 2009.

Appendix 9: Technical Evaluation Report: CCST Challenges, Sandia National Laboratory, April 2012



Sandia National Laboratories

Operated for the U.S. Department of Energy by
Sandia Corporation

P.O. Box 5800 Albuquerque, NM 87185-0832

Ken Bernier
Sam Holmes

April 19, 2012

Susan Hackwood
Executive Director
California Council on Science and Technology
1130 K Street, Suite 280
Sacramento, CA 95814-3965

TECHNICAL EVALUATION REPORT: CCST CHALLENGES

The California Council on Science and Technology (CCST) report identifies many of the pertinent technological issues associated with Managed Access Systems. At the request of CCST, Sandia National Laboratories offers the following information about technical challenges for managing access to wireless devices.

1. A Technical Evaluation is conducted as part of the Sandia National Laboratories/New Mexico (SNL/NM) wireless approval program for most wireless devices entering classified work environments.
2. During review of the CCST Report on the Efficacy of Managed Access Systems to Intercept and Special Report: Inmate Cell Phone Use Endangers Prison Security and Public Safety, additional input is provided to help look at this problem from a technical perspective outlining the challenges Sandia National Labs has experienced with similar issues.
3. Some special program testing and independent evaluations have been completed by various organizations affiliated with the federal government over the past 10 years. Many of the reports are classified and hard to get hold of for review purposes. What is known, is that most wireless devices use various frequency bands for the various services offered by mobile computing devices today. For example, the ability to deny and defeat wireless devices today are much more complex due to the various frequency bands associated with each particular device that is manufactured and purchased for the consumer.
4. An anecdotal sampling of the complexities associated with this issue may be reviewed in signal analysis screen captures with one particular device, sold by one manufacturer, of a mobile computing device in Figures 1 through 6 below. These screen captures illustrate the differences between one mobile computing device with phone, internet, email, text messaging, Bluetooth, and receive web page capabilities.
5. More complex problems come from satellite phone subscribers. These signals are much more complex to capture due to the nature of the satellite phone transmitting and receiving in an upward and downward angle. Two-way paging devices also pose problems because the devices transmit at low power levels and are more difficult to monitor.

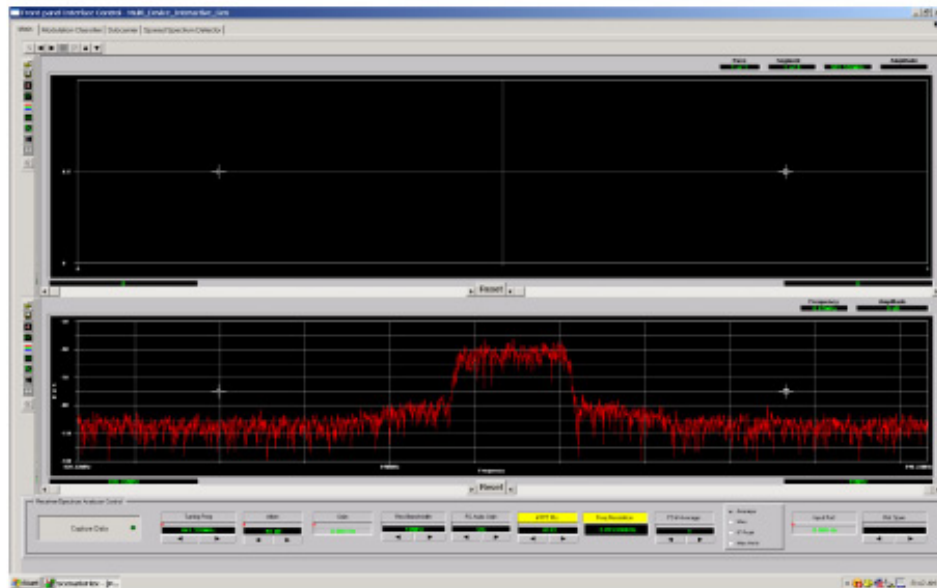


Figure 1. Phone transmission at 2 meters 841 Mhz -55dBm 1 Mhz BW

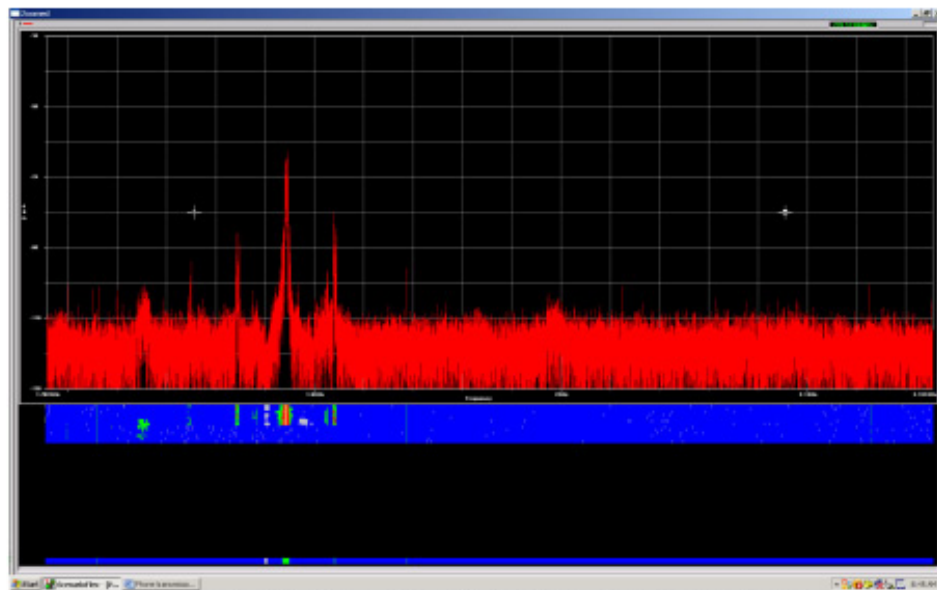


Figure 2. Internet Connection at 2 meters (5 second burst) 1.85 Ghz -75dBm

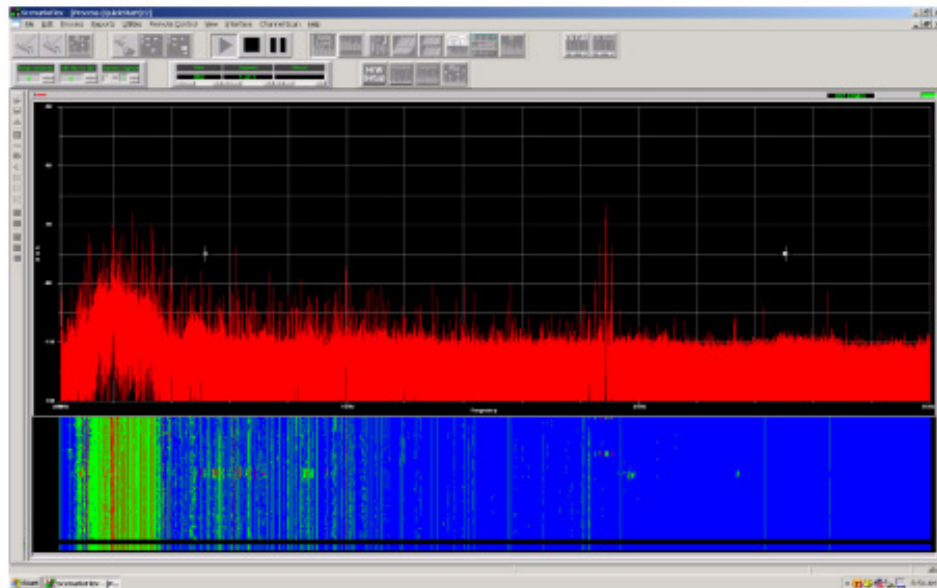


Figure 3. E-mail transmission 2 meters (5 second burst) 1.85 Ghz -75dBm

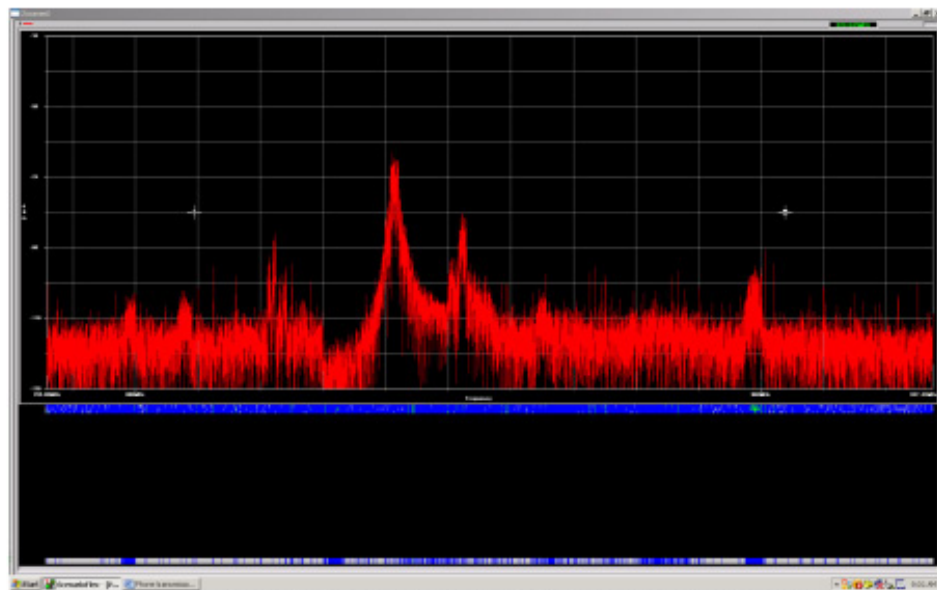


Figure 4. Transmitting a text message 2 meters (5 second burst) 841 Mhz -65dBm

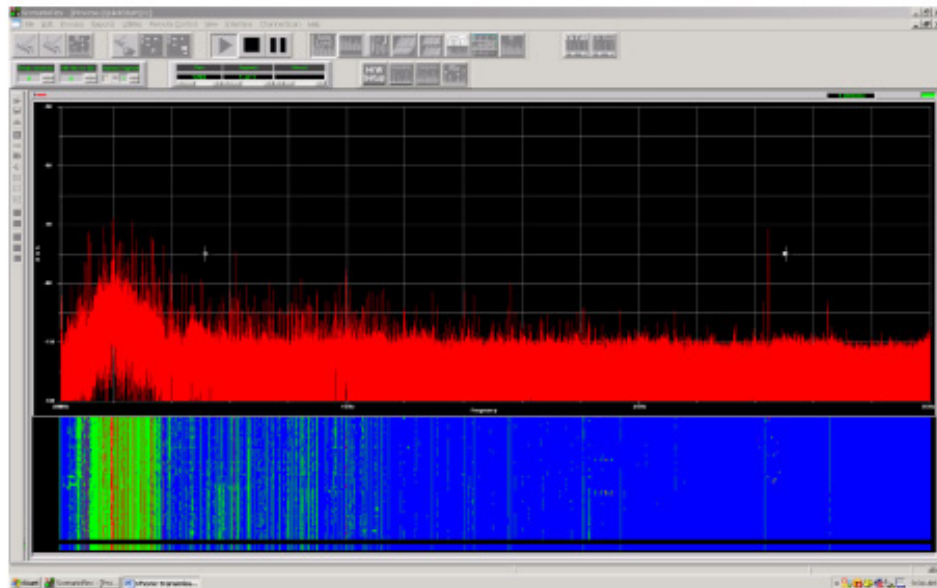


Figure 5. Searching for Bluetooth Connection 2.4 Ghz -88dBm

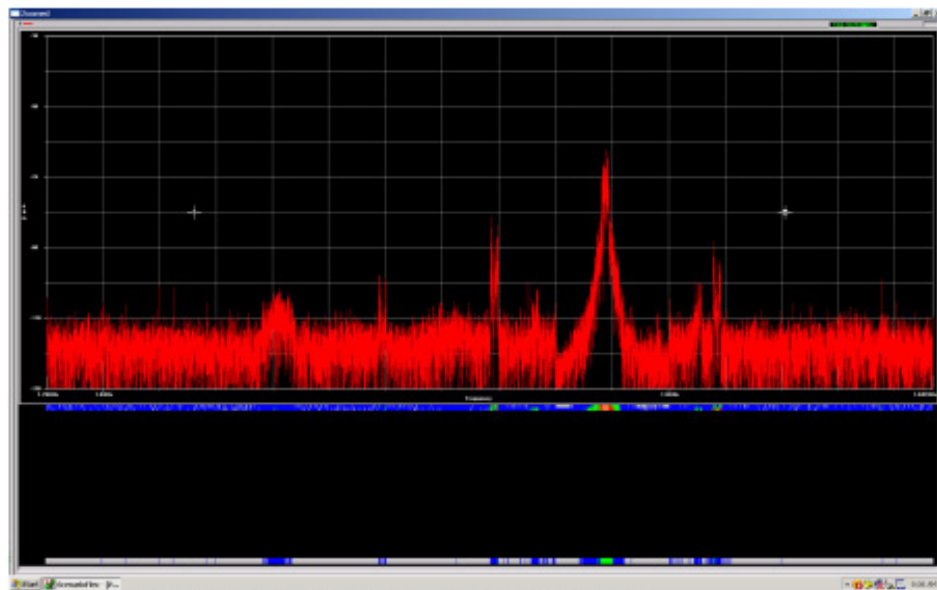


Figure 6. Receiving web page 1.8 Ghz -65dBm 10 Mhz BW

Evaluation Method: After operating signals are established, computer workstations are configured using various components. An RF analysis of the various workstation configurations are established to determine if any emanations are present.

Observations and Conclusions: As technology advances continue, additional problems will continue to surface. Issues such as GPS tracking, geolocation, wireless to wireless cloning, and RCC model devices are some additional risks that may be encountered at correctional facilities across the country.

Highly developed technologies are being developed to locate transmitters. Infinity and Air Patrol/Zone Defense have been used to pick up, triangulate, direction find, locate, and confiscate devices. See <http://airpatrolcorp.com/products/wi-fi-and-cellular-intelligence-solutions.php> for a video demonstration.



Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND Number: 2012-3332 P.



Bibliography - Source Documents

Legislative Request Letter to CCST Requesting a Study on Technology to Prevent Cell Phone Use in California Prisons

Request Letter to CCST from Senators Alquist, Hancock, Kehoe and Padilla, July 7, 2011

Letter From Senators to CDCR Secretary Matthew Cate

Letter to Matthew Cate,

November 6, 2011

CCST Contraband Cell Phones in Prisons Letter to Senators

Letter to Senators,

October 28, 2011

State of California Department of General Services

(IFB) Invitation for Bid - Inmate Ward Telephone System and Managed Access System Services Report

California Technology Agency, July 7, 2011

Bid RFI 10-001 - Cell Phone Interdiction: Shawntech Communications Pilot Response (Bid)

April 2011

Addendum to the Inmate/Ward Telephone System and Managed Access System Invitation for Bid (IWTS/MAS IFB)

IWTS Call Analysis - California Department of Corrections and Rehabilitation

Daily Phone Analysis (March 11-15, 2011)

March 2011

C5 System - Testing Results for CDCR SOL Facility

March 2011

Inmate Ward Phone System

Inmate Ward Telephone System - Solano State Prison Overall Call Volume 2009-2011

March 2011

SOL - Facility 1 - Daily Phone Analysis

March 2011

Comparing Inmate telephone use for Yard 1 against Yards 2 through 3 for the last 26 days

SOL Total Number of Completed Calls 2009 through 2011 By Day of Week (2/18 – 3/16/11)

SOL Take Nightops by Provider (March 24, 2011)

U.S. Department of Commerce

Contraband Cell Phones in Prisons: Possible Wireless Technology Solutions

December 2010

Office of the Inspector General

Special Report: Inmate Cell Phone use Endangers Prison Security and Public Safety

Office of the Inspector General, 2009

Articles

Inmates Harass Victims via Facebook

The Associated Press, November 21, 2011

Background Materials

Cell Phones in Prison

By: Tim Vice, Cell Phone Interdiction Manager, California Department of Corrections and

Rehabilitation

Bureau of Prisons: Improved Evaluations and Increased Coordination Could Improve Cell Phone Detection

September 2011

Electronic Searches of Bureau of Prison Staff Protocols

Glossary

3GPP	Specification writing body for the GSM (including GPRS, EDGE, UMTS and LTE) family of standards.
3GPP2	Specifications writing body for the CDMA (including CDMA2000) family of standards.
Bluetooth	Short-range RF communications protocol standardized by the Bluetooth Special Interest Group (SIG).
Circuit-Switched (CS)	A telecommunications network that requires a dedicated path between the two nodes.
Code Division Multiple Access (CDMA)	One of two major cellular radio technologies. Invented by Qualcomm and used primarily by Sprint and Verizon Wireless in the United States.
CDMA2000	Advanced CDMA standard adding high-speed data capabilities to the CDMA standard.
Cell Phone	Radio-telephonic instrument used to make telephone calls, send and receive text (SMS and MMS) message, or send and receive data using licensed radio spectrum.
Contraband Cell Phone	Cell phones in the unauthorized possession of inmates in the confinement of prisons.
Cell Phone Carrier/Provider/Network	Company, which operates a cellular network, such as AT&T Wireless, Sprint, T-Mobile and Verizon Wireless in the United States.
Enhanced Data Rates for GSM Evolution (EDGE)	High-speed data capability for GSM networks. Typically referred to as a 2.75G network standard.
General Packet Radio Service (GPRS)	High-speed data capability for GSM networks. Typically referred to as a 2.5G network standard.
Global System for Mobile Communications (GSM)	One of two major cellular radio technologies. Primarily used by AT&T Wireless and T-Mobile in the United States.
Institute of Electrical and Electronics Engineers (IEEE)	Specifications writing body for the WiMax family of standards.
Internet Protocol (IP)	Primary protocol for transferring data packets on the Internet.
Invitation for Bid (IFB)	Formal request for proposal by the California state government.
Licensed Frequency Bands	Bands of the RF spectrum set aside for licensed operation only. Cellular frequency bands, TV and Radio transmission frequencies are examples of licensed frequency bands. An FCC license is required to transmit in licensed frequency bands.
Long Term Evolution (LTE)	All-IP advanced wireless standard from the 3GPP specifications body. Can refer to both LTE, and LTE Advanced services.
MicroSD Cards	A flash memory card used in cell phones measuring only 11mm x 15mm.
Managed Access System (MAS)	A cellular network system which manages user access to cellular networks by preventing unauthorized users from connecting to a public cellular network, while allowing authorized users to connect to public cellular networks.
Packet-Switched (PS)	A telecommunications network that utilizes a shared-path between nodes, segmenting traffic into packets for transmission between nodes.
Personal Area Network (PAN)	Short-range, low-power wireless data networks used for the transmission of (typically) small amounts of data. Examples of PAN technology include Bluetooth and Zigbee.

Unlicensed Frequency Bands	Bands of the RF spectrum set aside for unlicensed operations. The Industrial, Scientific and Medical frequency bands are examples of unlicensed frequency bands. An FCC license is not required to transmit in unlicensed frequency bands as long as certain regulations, such as power levels, are observed.
Wireless Fidelity (Wi-Fi)	Most common standard of Wireless Local Area Network technology. Defined by the IEEE 802.11 family of standards.
WiMax	All-IP advanced wireless standard from the IEEE specifications body. Can refer to both WiMax, and WiMax Advanced services.
Wireless Local Area Network (WLAN)	Medium-range (up to 100s of meters) wireless data networks used for the transmission of large amounts of data. An example of WLAN technology is Wi-Fi.

Cover Photo Credits
© iStockphoto.com/ccstaccountant

Production Team
CCST Executive Director, Susan Hackwood
Project Team
Cover, Layout and Design, Sandra Vargas-De La Torre

