ManTech
International Corporation ®

Preventing Contraband Cellular Phone Use in Prisons

A Technical Response to NTIA

June 11, 2010

ManTech International Corporation
Luis Jose Cruz-Rivera,
Luis.Cruz-Rivera@ManTech.com

Antonio Quevedo,
Antonio.Quevedo@ManTech.com

Contents

1. Overview

From correctional facilities within the United States (U.S)[1] and throughout the world to homeland defense and scenarios taking place on battlefields,[2] illicit cellular phone use and unauthorized mobile data systems access is impacting mission safety at many levels. As evidenced by recent congressional activities[3] and the National Telecommunications and Information Administration's (NTIA)[4] Notice of Inquiry (NOI) regarding technical solutions to detect and prevent illegal use of cellular phones in correctional facilities, this problem is a growing threat to the security of our nation and its citizens.

Too often, solution are designed to control threats, such as the growing cellular contraband problem and other major safety concerns, focus on the technology component[5], and fails to consider the appropriate combination of skills, processes, and technologies to enable a comprehensive solution. In the case of contraband of cell phone use within correctional facilities, the solution lays in the architecture, addressing and combating the root cause of the problem. The effective use of technology can combine intelligence gathering with analysis to support the security mission. Effective operating scenario knowledge, decision-making capabilities, and goal attainment need to ultimately control and deny this contraband issue.

Commercial off the shelf (COTS) standalone systems do not offer a complete and satisfactory solution to the contraband cell phone challenge detailed in the NTIA request. Consideration of unified operational requirements, concepts of operations and functional requirements must be applied to the selection of available systems or development of an effective system of systems appropriate to address the mission space. This facilitates the deployment of an intelligent architecture for centralized and regional environments alike with a comprehensive affordable solution.

The commercial market space has recognized this disparity and as the NTIA NOI identifies several point solutions or technologies have been developed within the current regulatory environment to address the known cellular contraband issues. For the purposes of this paper these solutions fall into two general categories – active radiofrequency (RF) systems and passive RF systems. While there are hybrid scenarios (a solution using both active and passive RF), this document will focus only on the solutions that fall into the active RF category and the passive RF category; hybrid solutions are excluded from this analysis. Furthermore, this document intends to elucidate a comprehensive approach for managing the operational data needs of

[1] Kevin Johnson (November 20, 2008), *Smuggled cell phones flourish in prisons*, USA Today

[2] http://www.globalsecurity.org/military/intro/ied-iraq.htm

[3] Safe Prisons Communications Act. US Senate Bill, S.251

[4] National Telecommunications and Information Administration, Notice of Inquiry, No. 100504212–0212–01]

[5] *GAO-09-888 , DOD Needs to Strengthen Management of Its Statutorily Mandated Software and System Process Improvement Efforts*, September 2009

several layers of the U.S. Government and other key stakeholders affected by illicit use of cellular phones in prisons.

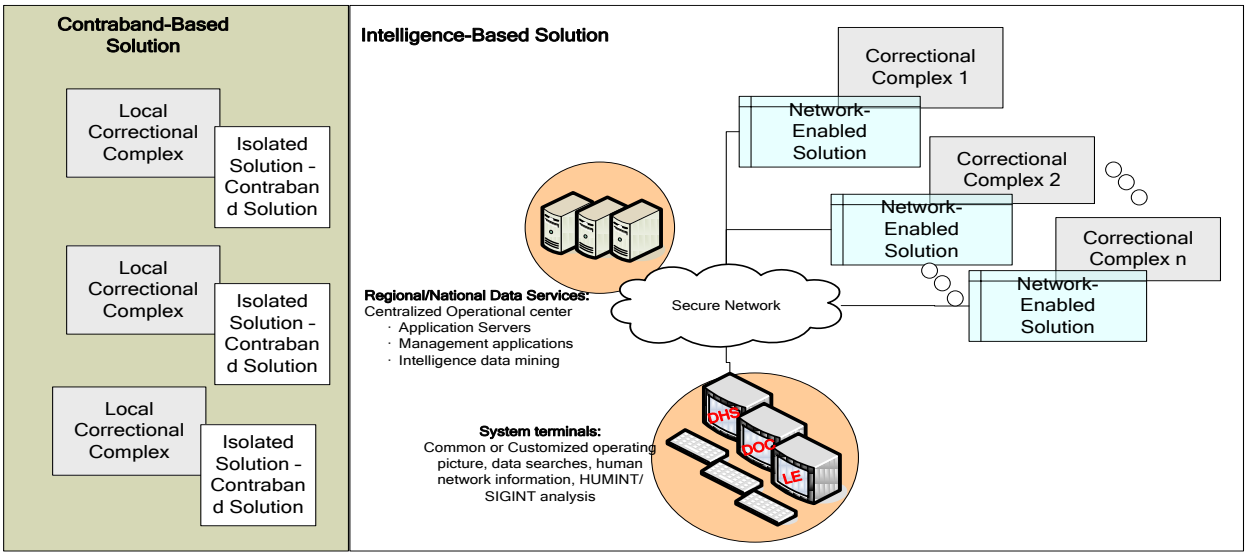

Figure 1. Contrast between the Contraband-Based Solution and Intelligence-Based Solution

This document will discuss the two solution types and provide details regarding several technology and deployment considerations to address the architecture of the solution. Figure 1 depicts the two mission areas in which all of the possible solutions fall - contraband-based solutions and intelligence-based solutions. The contraband-based solution addresses the short-term need for denial by jamming or detection and monitoring for manual control. The intelligence-based solution provides varying capabilities of C3I (Command, Control, Communications, and Intelligence) interface and allows stakeholder operations to address criminal or other activities of interest within stakeholder jurisdictions. This capability can bridge other additional security needs to the solution, thus enabling the correctional community to utilize data sharing with law enforcement and judicial stakeholders to maintain a holistic view of criminal network communications and contraband management activities within the target locations. The level of metadata attainable in these transactions provides a large data-mining capability, which can interface with other operating scenario data sources and provide a new appreciation for connection networks.

Within the scope considered by NTIA,[6] solutions to this problem will serve the following primary stakeholders:

- Prisons and correctional institutions that want the technology to solve the problem
- Commercial operators who have paid millions and in some cases billions of dollars for spectrum and equipment and do not want their coverage of valid users impacted
- The general public who wants a solution to stop the criminal activities but without impact to their use of devices on the outside of the correctional institution location

[6] National Telecommunications and Information Administration, Notice of Inquiry, Docket No. 100504212–0212–01

Other stakeholders include:

- State and local law enforcement agencies requiring increased insight and awareness of activities linked with illicit communications
- Department of Homeland Security (DHS) data fusion centers, Department of Justice (DOJ), National Institute of Justice (NIJ), Drug Enforcement Administration (DEA), and other law enforcement (LE) entities
- Government and industry associations responsible for overseeing the use of spectrum and wireless technology that want a solution that can operate within the boundaries of the law and regulations

The opportunity to solve this problem using technology addresses a broad market segment, which also needs to coexist with other security efforts and data-sharing initiatives among the stakeholders. Strategic acquisition and integration work will be critical to deploying a given solution in order to avoid reengineering of design due to technology fluctuations, obsolescence, and total cost of ownership. If a rigorous solution development process is not followed, correctional institutions run the risk of committing and expending unnecessary resources and funds resulting to system implementation defects, technical capability gaps, and system suitability inadequacies within a constantly changing wireless environment.

2. Cellular Technology Developments and Practices

The evolution of technology in the cellular industry produces an ongoing push toward enhancing products and solutions that challenge any currently deployed solution's effectiveness. With the significant growth of data transmission demand, the networks have transformed the accessibility, adoption, and utility of data and multimedia services in to their provision roadmap. The evolutionary trends and requirements of this industry bring in a significant higher risk profile to obsolescence and performance. As device manufacturing and technologies mature, so do the mobility and bandwidth requirements on the commercial networks and the complexity of the authentication protocols used by both passive and active solutions. Additionally, with the advent of MIMO (multiple input, multiple output) technology and the diversity of frequencies used for mobile telecommunications, the future data services (wherein voice is an application of data) for cellular phone detection and control will have significant new challenges as the value of the contraband and its trafficking is expected to also increase. Other innovations which can change the solution value proposition:

- ***Wide Band Detection and signal processing***. The Wideband detection and signal processing technique uses acoustic signatures for direction-finding and tracking of large devices/vehicles. Low complexity algorithms allow for implementation as a real-time function that can be integrated into existing infrastructure.
- ***Software-Defined Radio.***[7] Software-defined radio (SDR) allows a single wireless device to support a wide range of capabilities previously available only by integrating multiple radio components. Software-programmable radios allows easy changes of the radio fundamental characteristics such as modulation types, operating frequencies, bandwidths, multiple access schemes, source and channel coding/decoding methods, frequency spreading/dispreading

[7] http://www.wirelessinnovation.org/page/What_is_SDR

techniques, and encryption/decryption algorithms. These new features and capabilities, when added to existing infrastructure, will not require major new capital expenditures to address future needed enhancement.

Security Risk of Carrier Network Evolution

Current technology changes, such as providers migrating to different broadcasting protocols, evolving standards, and new spectrum usage, alter the cellular communication market landscape. Next generation mobile phone standards are imminent. By 2012, it is expected that many cellular phones will meet LTE, WiMAX, and ultra-wideband (UWB) requirements. This multitude of existing and evolving standards, as outlined in Table 1, coupled with the need to react quickly to market requirements, radically changes the utility profile of any current single-point solution investment.

Table 1. Mobile phone standards

Specification	Wi-Fi ultra-wideband	802.11a/b/g	802.11n	Wireless broadband (WiBro)	Mobile WiMax (802.16—2005)	3G LTE (cellular WAN)	Digital Video Broadcasting—Handheld	Digital Video Broadcasting—Terrestrial
Application	High-speed local interconnect, wireless USB	Medium-speed LAN	High-speed LAN	Mobile wireless access	Mobile wireless access	Mobile data/voice	Mobile TV	Mobile TV
Range	10 m	80 m	50-150 m	1-5 km	1-5 km	1+ km	Broadcast	Broadcast
Rate	480 Mbps	11 Mbps (b), 54 Mbps (a/g)	100-600 Mbps	3-50 Mbps (downlink)	63 Mbps (downlink)	100 Mbps (downlink)	384 Kbps	7 Mbps
Frequency	3.1-10.6 GHz	2.45/5.8 GHz	2.45/5.8 GHz	2-6/2, 3 GHz	2-6/2, 3 GHz	1.25/2.2/5/10/20 GHz	0.8 MHz, 1.6 GHz	0.8 MHz, 1.6 GHz
Modulation	Orthogonal frequency division multiplexing	Direct-sequence spread spectrum/ complementary code keying, carrier sense multiple access, orthogonal frequency division multiplexing	Carrier sense multiple access, orthogonal frequency division multiplexing	Orthogonal frequency division multiple access	Orthogonal frequency division multiple access	Orthogonal frequency division multiple access/single carrier frequency division multiple access	Orthogonal frequency division multiple multiplexing	Orthogonal frequency division multiple multiplexing

Table adapted from a figure provided by NXP Semiconductors.

In the correctional environment, as in other security areas, the stakeholder solution to the mission need must identify the activities and architecture elements that will minimize or eliminate the cellular technology migration risks. The solution's life cycle cost and maintenance models must account for these industry changes. Since use cases for high-end and mid-level mobile phones involve only a few simultaneous standards, it is believed that reconfigurable architectures that can simultaneously address the different communication standards would achieve significant savings. Ancillary equipment may require configuration changes due to the need to account for the increased power consumption resulting from RF tuning and combining RF distribution segments.

3. Available Technologies

In response to Notice of Inquiry issued by NTIA, the following cross-sectional capabilities can leverage detect, localize, jam, and control cellular systems and their potential for upgrading given migration of technology.

Correctional institutions have deployed passive systems. However, these systems do not yield the technical effectiveness and system suitability that stakeholders require for countering illegal cellular contraband use due the absence of operational resources required to deploy the technology.

- Passive
  - Manual inspection, searches with handheld devices
  - Trained K-9 units
  - RF fixed and mobile sniffers/detector arrays
    - Manually operated – minimally effective with moderate to high operational costs, depending on size of institution footprint
    - Autonomous – moderately effective with moderate operational costs

Active cellular deterrent systems provide technical and operationally effective means of efficiently eliminating the use of cell phones within correctional institutions. This whitepaper will focus on the implementation considerations NTIA to feedback to Congress as effective means of countering cellular use without negatively affecting commercial wireless and public services (including 911 calls and other Government radio services) in areas surrounding prisons.

- Active (now eligible for procurement with legislation)
  - RF broadband jammers
  - RF notch/channel jammers
  - Managed access control systems
  - Integrated network control systems

General Passive Systems Response to NTIA NOI

System Operating Concept

1. Concept of Operation
   a. Passive detection systems generally search for radio frequency emissions within a region of interest and in some cases search for cellular modulated signals. Since the family of detectors is deployed as a series of micro-networks, general location information can be relayed to the proper stakeholders, thus enabling confiscation efforts. The general location's resolution is directly dependant on the number of detectors deployed; the more detectors that are deployed, the higher fidelity of the location function.
   b. Some passive detectors can log cellular activity information within their effective detection radius.
2. Infrastructure implementation considerations
   a. Ancillary equipment – Standard power distribution, local area network, and cellular support equipment may be used to deploy the system.
   b. Multiple systems per institution
      i. Passive detector systems requiring a surgical approach in deploying passive cellular phone identification and location system to help staff physically locate phones.
3. Impact to commercial and public services
   a. Passive detection systems do not impact the neighboring commercial networks.

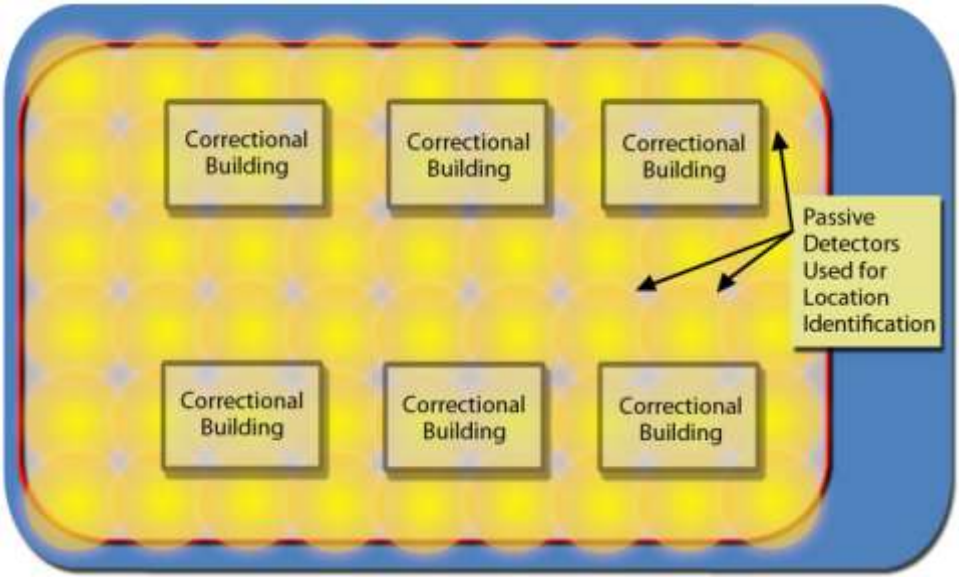

Figure 2. Passive Detectors in Correctional Institutions

4. Upgrade capability
    a. A passive detection system's upgrade capability is minimal. Passive systems requires field and support activities at each detector in order to upgrade to future communications protocols.
5. Response time required for upgrade and initial installation
    a. Initial installation
        i. A significant amount of construction is required to deploy the systems properly and provide a moderate level of resolution for cell phone locating.
6. Upgrade/installation disruptiveness
    a. Disruptiveness is typically heavy due the integration of multiple receivers along with the required ancillary equipment needed to support all receivers within correctional standard building requirements.

Cost Considerations

1. Architecture considerations
    a. The deployment of jammers requires typically two types of units– omni and directional antennas. Directional antennas help minimize the leakage of RF energy that radiates behind transmitters.
    b. System deployment generally connects all detectors over proprietary wired data network.
    c. Design considerations for vandalism influence detectors placement within the inmate living spaces.
2. Reoccurring costs
    d. Passive systems require continuous manpower to enable effective cellular phone search and seizure operations within the footprint, without compromising safety.
3. Variables affecting cost
    a. Size of institution
    b. Spatial fidelity of detection

c. Number of staff required to man the use of cellular phone detection technology and the search and seizure activities

4. System suitability given prison size
    a. Operates seamlessly, assuming the physical hardening infrastructure is protecting the systems

Technology Readiness

Passive detector systems utilize non-standard integrated equipment that has not been widely deployed in the U.S. and do not have reliability characteristics similar to the cellular industry standards.

General Jammer Systems Response to NTIA NOI

System Operating Concept

1. Concept of Operation
    a. A jammer system radiates RF energy within the spectrum of the carriers with a modulation scheme that disrupts service within a footprint, not allowing cellular phones to connect to the macro network. To reduce RF overlap into territories outside the correctional institution's footprint, the RF design needs to account for broadcast control. This can be accomplished by using numerous directional antennae and small isotropic antennae or other schemes to ensure that the footprint of the institution matches the RF effectiveness footprint.

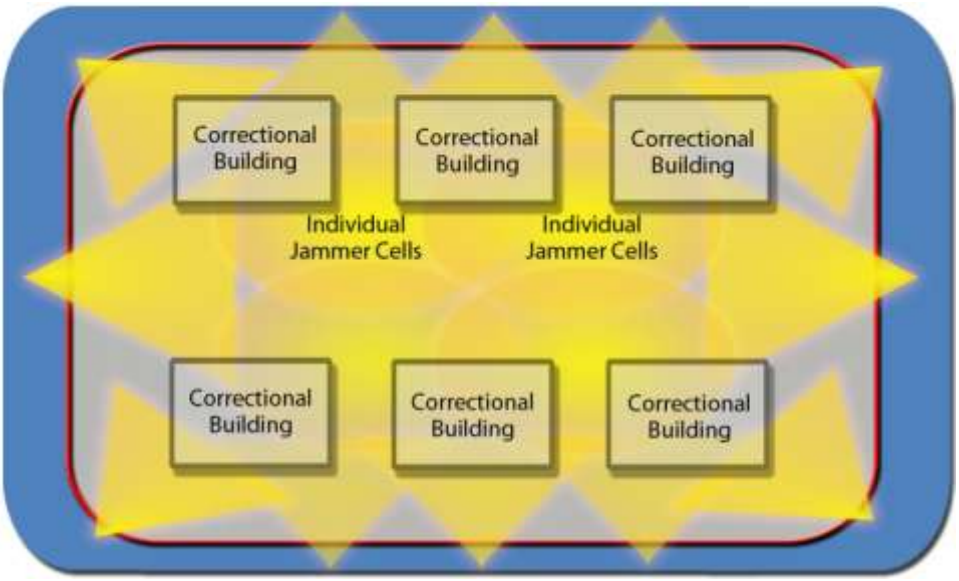

Figure 3. Jammer Cells

2. Infrastructure implementation considerations
    a. Ancillary equipment - standard cellular equipment is used to deploy the system. The use of repeaters provides coverage to areas where RF coverage is shadowed by building structures.

   b. Multiple systems per institution – jammer system deployment requires a surgical approach to ensure they are configured in a manner that minimally affects the footprint.
3. Impact to commercial and public services
   a. Jammer systems provide a challenge in bounding the effectiveness footprint due to the fact the RF does not drop off immediately, but rather at a 1/R^2 rate.
   b. A jammer system does not allow cellular users the ability to connect with public services using non-smart jammer systems. A smart jammer system, coupled with a passive system, can selectively jam and allow users access to communicate to the macro-network if the call is attempting to communicate with a public service provider, such as 911.
4. Upgrade capability
   a. A jammer system can be configured to adapt the changing cellular operational environments. Its adaptation can be modified at the component level, as opposed to changing out the entire system due to a given a change in the local cellular environment. Major components for modification would include power levels and modulation schemes.
5. Response time required for upgrade and initial installation
   a. Initial installation
      i. RF survey: moderate timeline required to ensure that construction code guidelines are followed and since the jammers will be distributed transmitters that will be within reach of the inmates
      ii. System & RF design based on survey data which includes the number of carriers, frequency block usage, installation topology, and material.(10 days)
      iii. Test & Evaluation planning and verification for system functionality and requirements verification (i.e., only effective within correctional footprint)
         - To be concurrent with long-lead procurement and 30 days after for data collection and report writing
6. Upgrade/Installation disruptiveness
   a. Disruptiveness is typically moderate to heavy due to having to integrate multiple transmitters along with the required ancillary equipment to support all of the transmitters

Cost Considerations

1. Architecture considerations
   a. The deployment of jammers requires typically two types of transmitters – omni and directional antennae Directional antennae help minimize the leakage RF energy that radiates behind transmitters.
2. Operational Cost Impacts
   a. A jammer system provides interference that affects both stakeholders within the correctional institution environment (wardens & staff). An Access Control System autonomously denies illicit cellular users requiring minimal operational support.
3. Reoccurring Cost
   a. A jammer system would require dedicated power and minimal support to update modulation schemes and inspect system integrity with its supporting infrastructure.
4. Variables affecting cost

a. Number of carriers in a given footprint; 3G and 4G service available
b. Number of areas RF shadowed

5. System suitability given prison size
    a. A system being deployed within an external community, traffic, or other industries.

Technology Readiness

Jammer systems utilize non-standard integrated equipment that has not been deployed in the U.S. and generally do not have reliability characteristics similar to the cellular industry standards. Due to the absence of knowledge available about illicit enterprises, jamming is not foolproof – especially with MIMO implementation in new generation handsets and communication standards, some phones may be able to work through jamming using software that filters out jamming signals. In the end, jamming may provide a false positive success rate, as there is little ability to verify if phone can communicate outside of the prison walls.

General Access Control Systems Response to NTIA NOI

System Operating Concept

1. Concept of Operation
    a. An access-control system that leverages the cellular industry COTS equipment and couples it with modified routing software that selectively traps cellular phones. The system selectively allows authorized users to access the macro-network by having a database containing the users' cellular identification information (MIN, ESN, etc.). As seen in Figure 5 and 6, the subscriber's handset (based on locking to the local control channel) attempts to register in the VLR with normal handshake protocols. If the cellular phone is registered with the system, the system routes the user to the macro network; if not, the user is locked into the micro-network where it sends the user network busy signals when attempting a call.

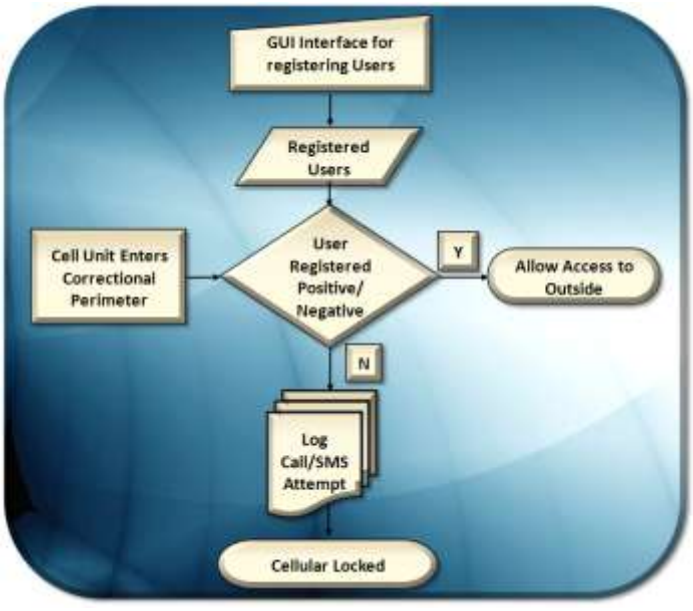

Figure 5. Access Control System Process Flow

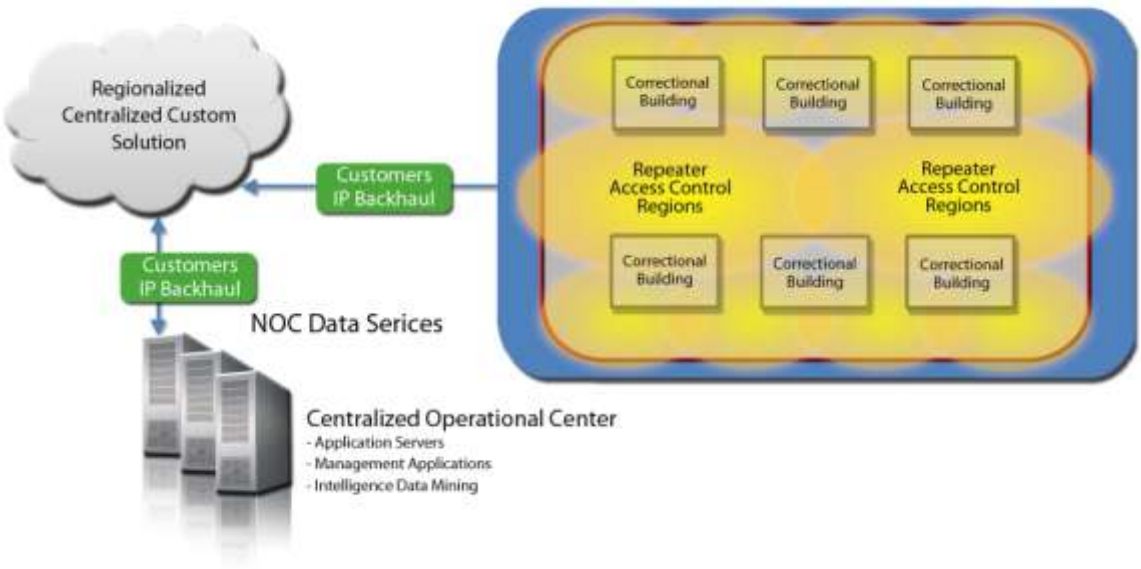

Figure 6. Access Control Systems

2. Infrastructure implementation considerations
    a. Ancillary equipment – standard cellular equipment is used to deploy the system. The use of repeaters provides coverage to areas where RF coverage is shadowed by building structures.
    b. Single system per institution – a core system is used at each institution
    c. Star networked-centralized solution
    d. Networked Operating Center (NOC)– centralized operating center is optimal for the users to update the authorized users' data base or change system settings. The NOC should be placed in a HQ like setting for use by proper management.
3. Impact to commercial and public services
    a. The access control system is designed to function within the macro-network if designed and tested to ensure the coverage footprint is within the correctional institution.
    b. The access control will not take a handoff of a cellular phone in use that is passing by the micro-network based on the software rules settings.
    c. The access control software provides all cellular users the ability to connect with public services

Upgrade Capability

1. Upgrade capability
    a. An access control system can be configured to adapt the changing cellular operational environments. Its adaptation can be modified at the component level, as opposed to changing out the entire system due to a change in cellular local environment. The technology utilizes industry communications handshakes that do not disturb quality of service beyond the effective zone.
2. Response time required for upgrade and initial installation
    a. Initial installation time considerations

i. RF Survey
ii. System & RF Design based on survey data (# of carriers, frequency block usage, installation topology, and material.
iii. Procurement of long lead items
iv. Test & Evaluation planning and verification for system functionality and requirements verification (i.e., only effective within correctional footprint)

3. Upgrade/Installation disruptiveness
    a. Disruptiveness is typically minimal because a typical installation will be centralized and does not require the movement of inmates

Cost Considerations

1. Architecture considerations
    a. Access control systems require leading line items involving software licensure, BTS, and Ancillary. Leveraging a centralized solution provides an architecture that minimizes line item cost of licensing.
2. Operational cost impacts
    a. An Access Control System autonomously denies illicit cellular users requiring minimal operational support from personnel. Capital costs are higher than most jammer and detector systems. Ancillary and construction costs for full coverage of a complex or large facility is significantly lower than other solutions.
3. Reoccurring costs
    a. An access control system would require dedicated power and minimal support to update and data mine information from the system's log files. Intelligence support would be the only reoccurring cost that the user would incur.
4. Variables affecting cost
    a. Number of carriers in a given footprint
        i. 3G and 4G service available
    b. Number of areas RF shadowed
5. System Suitability Given Prison Size
    a. Centralized solution not requiring significant construction
    b. Centralized control center that is tamper proof

Technology Readiness

The access control system utilizes enterprise level cellular industry equipment that has a robust reputation in providing high reliability and availability statistics.

4. Key Architecture Considerations

Stakeholder Groups

Within the scope considered by NTIA,[8] solutions to this problem will serve the following primary stakeholders:

[8] National Telecommunications and Information Administration, Notice of Inquiry, No. 100504212–0212–01]

- Prisons and correctional institutions that want technology solutions to the problem
- Commercial operators who have paid millions, and in some cases billions, of dollars for spectrum and equipment who do not want their coverage of valid users impacted
- The general public who wants a solution to stop criminal activities but without impact to their use of devices on the outside of the correctional institution location.

Other stakeholders include:

- State and local law enforcement awareness of activities linked with illicit communications
- DHS data fusion centers, DoJ and NIJ, DEA, and other law enforcement agencies
- Government and industry associations who oversee the use of spectrum and wireless technology want a solution that can operate within the boundaries of the law and regulations

This opportunity to insert technology addresses the correctional market segment, which strategically operates with other security efforts and data sharing initiatives throughout DOJ and other agencies such as DHS. Strategic planning, acquisition, and integration work will be critical for the deployment of a given solution in order to avoid reengineering of design due to technology fluctuations, obsolescence, and reliability/cost issues. In such a case that rigorous solution development process is not followed correctional institutions run the risk of committing and expending a myriad of funds as ballooning costs would be incurred due to defects of system implementation, technical capability gaps, and system suitability in a changing wireless environment.

Requirements Based Design

As described in Section 1, the risk of illicit or mal-intentioned use of the wireless spectrum is recognized[9] and the stakeholder group is not exclusive to just correctional institutions and jails. Other entities tied to public safety, law enforcement, and the homeland security domain also have a vested interest in eradicating the problem in prisons, as well as gaining intelligence from the communication vector. Besides correctional environment, many other security sensitive or critical scenarios exist in support of law enforcement and homeland security, which can benefit from these advances in technology, process, and policy. Furthermore, investments can support other related needs (i.e., interoperability and asset tracking), thereby increasing the community's value for the application.

By generating a more transparent and user-suitable solution, stakeholders can mitigate illicit communications and generate the knowledge base to identify other higher-level schemes of contraband or criminal activities. The acquisition or solution development process used to initiate the local solution should consider applicable operational scenarios at the local, state, or federal level. These derived requirements will detail the operational test cases in order to assure sought value proposition. Ultimately, in collaboration with law enforcement and the established metric delivery systems, correctional managers can allow solution operators to stop or manage illicit communications though a network interface. Sample requirements are as follows:

- Cover all types and brands of cellular phones and all available networks

[9] Press Release, *Senate Passes Hutchison Bill to Prevent Inmates from Using Smuggled Cell Phones*, Oct. 5, 2009, *available at* www.commerce.senate.gov.

- Cover the entire region of interest and not interfere with legitimate phone use
- Not generate nuisance alarms due to legitimate phone use in nearby areas
- Allow monitoring of the entire facility or collection of facilities from a central location
- Be operable by minimally-trained personnel while operating all day, everyday
- Fully comply with all FCC regulations
- Support data mining and ODBC application
- Be CALEA[10] compliant
- Detect and locate voice calls, text and picture messages, and data sessions
- Verification of functional and operational requirements through testing

Trade Studies

Any solution deployment configuration intending to address illicit cellular phone usage will depend on the targeted application and the geographic coverage requirements. Upon reviewing the existing commercial off the shelf (COTS) capabilities (market review included data from airPatrol, ITT, EDO, Tecore Networks, Binj Labs, and Vanu) and defining the continued development need, the measures of effectiveness can be used to determine the configuration of the solution needed for a given mission space to include different correctional scenarios, priorities, or budgets. This paper excludes these measures.

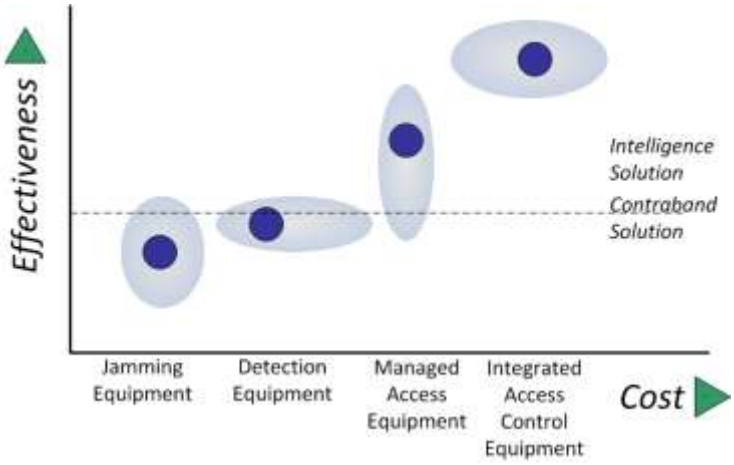

Figure 4. Significant Differences in Overall Effectiveness of Alternatives

If the definition and selection of risk profile is based on operational scenarios, the analysis allows for the identification of suitable source solution maps to establish the relationship of effectiveness against the relative cost of each technology type. Figure 1 depicts the systems for both the contraband-based solutions and the intelligence-based solution sets.

In this case, the stand-alone jamming, the jamming by distributed antenna network, and the detection solutions exist in a by-institution, stand-alone solution, or array deployment for which a linear relationship between effectiveness and costs exist. Depending on the featured set and

[10] CALEA- Communications Assistance for Law Enforcement Act. Congress enacted CALEA on October 25, 1994. CALEA was intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities. http://www.fcc.gov/calea/

robustness of the packaging (e.g., enclosures: sheet metal versus Nema-4), similar effectiveness have differing price points. Detection equipment can be either location-only equipment or can decode the RF detection and collect call data. The intended use defines the complexity of the algorithm and hardware. This technical solution bridges the intelligent solution divide but has a higher cost of ownership and susceptibility to tampering or vandalism. Furthermore, the cost distribution is affected by the level of resolution for detection, which is proportional to the number of detectors in the array. These factors result in high cost variability. Managed access has a higher comparative cost with less variability, as it is based on the commercial arrangement and use of communication frequencies and technologies. In rural settings, not all national providers have coverage, thereby reducing the capital equipment cost. Lastly, the integrated access control solution, which has a similar function as the managed access solution but provides a high effectiveness and data mining capability, which can be customized depending on operational need, risk, and available solution requirements in the target facilities. While this has an initial higher cost for deployment, there are several investment reuse possibilities with interoperability extensions and CALEA on the short list.

Top-Level Architecture

The cost-benefit question depends mainly in the deployment volume and required function of the common operational requirement for security over the spectrum of service provision technologies. This results in addressing the user-specific operations by the solution architecture chosen to address the specific mission. In all cases, the solution's capability will control, detect, and/or deny the illicit communications without compromising human resources or other legitimate communication channels or rights of legitimate use of these communication channels.

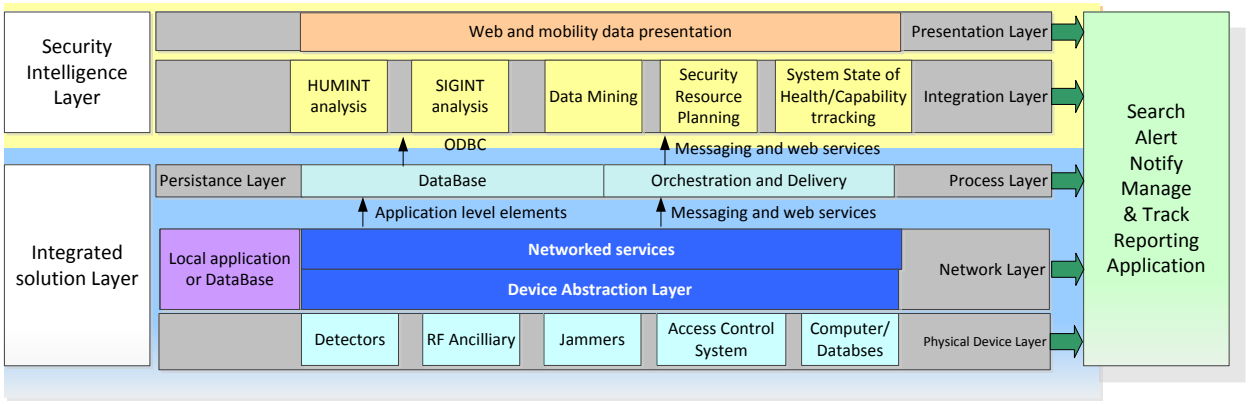

Figure 5. Functional Layer breakdown of proposed architecture

The technical solution needs to support a wide range of communication technologies and frequencies. By generating trend and operational intelligence from these illicit acts stakeholders such as security, agencies can monitor the physical device layer and infrastructure. Within the integrated solution layer, the network layer addresses the network connectivity and scenario data sharing to enable various improvements in calibration, system resiliency, and customization. For example, when commercial providers' change their control frequency schema, the system needs to have operational control measures of health status to identify when new optimization procedures or new programming are needed. Subsequently, the data gets stacked and manipulated to feed specific applications or data views. As the information leaves to the security

intelligence layer, data and other attributes and files can be filtered into the integration layer. Besides stand-alone monitoring at the integration layer, processed data is pushed through the designated user interface point. This interface accounts for authentication, network edge security, and the reporting functions. All of these layers feed the application and the project control or knowledge management scheme.

Once functional requirements are established, the basic data architecture and solution set can be duplicated and tailored over multiple sites, as needed. Site implementation will vary based on requirements management, software, data products, and other site constraints such as RF engineering and planning. With the exception of the jamming devices, other intelligence alternatives, such as the managed service devices and the detection systems, can be coordinated with the commercial service providers thereby not affecting commercial signals.

5. Summary

The cellular contraband problem in the correctional environment already has active (excluding jammers) and passive solutions in place. Jamming as a solution may be needed as a part of the solution to certain security scenarios. The correctional system can increase the benefit of technology insertion by structuring an architecture that can be leveraged across many institutions. Centralizing control and data management, even when operations are site-specific, can minimize cost by networking, systematic planning, and systems operations. Proper systems engineering and data management design can help extend the infrastructure investment while focusing reengineering and design efforts to address technology solutions.

By utilizing functional requirements, establishing structured deployment architecture, and ensuring proper systems engineering support (e.g. RF engineering, verification and validation) stakeholders can support a robust multi-jurisdiction plan for deploying the correct solution.