EXHIBIT C
REQUEST FOR INFORMATION DOC-16-079

PROPOSAL FOR INMATE ELECTRONIC COMMUNICATION SYSTEMS
We exist to **SERVE** and **CONNECT** to make our world safe.

An RFI Solution Prepared for:
Virginia DOC
Inmate Electronic Communication Systems
Due March 28, 2016 10:00AM EST

Presented to:
Peter Batley, VCO, CPPB
Procurement Manager
Virginia DOC
6900 Atmore Drive
Richmond, Virginia 23225

Presented by:
**Adam Mercer**
National Sales Manager - DOC
Securus Technologies, Inc.
14651 Dallas Parkway, Suite 600
Dallas, TX 75254
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>COVER LETTER</td>
<td>2</td>
</tr>
<tr>
<td>COMPANY BACKGROUND</td>
<td>6</td>
</tr>
<tr>
<td>INMATE TELEPHONE SYSTEM OVERVIEW</td>
<td>12</td>
</tr>
<tr>
<td>KIOSKS / TABLETS OVERVIEW</td>
<td>90</td>
</tr>
<tr>
<td>MANAGED ACCESS SYSTEMS (MAS) OVERVIEW</td>
<td>111</td>
</tr>
<tr>
<td>RECOMMENDATIONS</td>
<td>120</td>
</tr>
</tbody>
</table>
March 28, 2016

Mr. Peter Batley, VCO, CPPB
Procurement Manager
Virginia DOC
6900 Atmore Drive
Richmond, Virginia 23225

RE: Request for Information DOC-16-079 Inmate Electronic Communication Systems

Dear Mr. Batley,

Securus Technologies, Inc. (Securus) appreciates the opportunity to submit our response to the Virginia Department of Corrections’ (DOC) Request for Information (RFI) – DOC-16-079 for Inmate Electronic Communications Systems. We recognize that you have many choices to make regarding the technology that best promotes the safety and security of both your staff, and the inmates that you are charged to rehabilitate. We take this opportunity to educate you on our technology very seriously. Within the enclosed RFI response, Securus has presented information regarding the various technologies in which you have expressed interest. We look forward to visiting with you and presenting our solutions in an effort to help you determine the content of your future procurements and solicitations.

Securus’ predecessor organization was founded in 1986, and we have been providing correctional facility communications systems and other services for almost 30 years. We are headquartered in Dallas, Texas, and are currently serving more than 3,400 public safety, law enforcement, and corrections agencies and 1,200,000 inmates across North America. In the state DOC space, Securus currently provides service to 11 of the 50 DOCs in the United States. Our subsidiary, JPay, provides additional services to 33 of the 50 DOCs.

Securus is the leader in delivering technology solutions to civil and criminal justice agencies. This includes the deployment of the most widely used inmate telephone platform, the development of the broadest available investigative technology suite, and the installation of the most operational inmate tablets in the industry today. No other company can meet your needs and provide a better level of service than Securus can!

This RFI response contains detailed information about each of the technologies in which the DOC has inquired. A brief description is also included below:

**Inmate Telephone System Solution**

Securus believes that communications management is central to most correctional facility operations. It affects safety, revenues, and overcrowding, and has a direct impact on the
wellbeing of staff and inmates as well as family members and friends. The Secure Call Platform™ (SCP) call management system is the heart of our communications management solution. The system provides Securus clients with the benefit of operating on a centralized, digital network that is proven and reliable for agencies just like yours!

Over 2,200 federal, state, county, and municipal prisons and jails currently have the SCP installed, making it the world’s most deployed inmate telephone system. The SCP is a cloud-based and web-enabled platform with virtually unlimited capacity. It delivers an array of cost reduction and safety enhancement features that automate the management of the inmate telephone system. It also seamlessly integrates with other DOC systems to increase efficiency and reduce manual re-entry of the same data. In addition, so users are never saddled with old or outdated software, Securus releases updates to the system three to four times per year so that its partners are assured their system remains on the cutting-edge of technology.

Securus’ recording and monitoring system is fully integrated with the SCP solution, and provides secure recordings of inmate telephone conversations. The system is completely secure, allowing **ONLY** authorized personnel to listen to live or archived recordings.

The SCP allows for immediate, real-time monitoring of telephone calls in progress via any authorized computer workstation or mobile device with Internet access. The computer or device display presents the specific telephone location, inmate PIN, destination number dialed, city and state called, time and duration of call, any restrictions on the inmate or call, and the status of the communication. The system records the entire conversation from call acceptance to call termination. Recordings are stored on-line for immediate access for 12 months.

The platform will also empower DOC personnel to create a safer and more secure correctional environment by providing features that include a PIN-based system, three-way call detection, remote call forwarding, Crime Tip (anonymous, two-way communication), Covert Alerts (real time call and e-mail alerts), robust reporting capabilities, and compatibility with TDD/TYY technology.

**Locations Based Services within SCP**

The SCP supports Locations Based Services (LBS), which is an investigative tool that provides correctional facilities with the control and oversight needed to safeguard against cellular phone threats. LBS allows facilities to investigate the location of inmate calls to cellular telephones, receive real-time alerts based on where the call is placed, and find the location of a cellular telephone even if an inmate is not currently using it. LBS also delivers real benefits to the community in aiding in exigent circumstances such as Amber Alerts or Silver Alerts.
Tablets/Kiosk Solution
Securus holds a unique position within the inmate communications industry in that we currently own and operate two separate and distinct inmate tablet solutions. In addition to our in-house developed Securus SecureView Tablet, our recent acquisition of JPay allows us to provide services through the JPay Tablet. Both of the tablet solutions are unique in design and functionality, and provide Securus the ability to customize a platform that best fits our clients’ needs.

Our tablet solutions are proven, and are currently installed and successfully providing all communication, entertainment, and educational programs in County and State corrections environments across the United States. In fact, just as Securus has the most widely used inmate telephone system in corrections today; we also have more operational inmate tablet installations than any other vendor in the market.

Based upon our understanding of the DOC environment and the requirements as stated in this RFI, we have elected to respond with our JPay Tablet solution. The JPay Tablet solution and pricing model has been tested and proven in a State corrections environment. JPay currently provides services in over 30 State DOCs, and the number of DOCs that are electing to implement the JPay Tablet solution is growing continually.

We are also in the process of integrating many of the advanced features from our Securus SecureView Tablet into the JPay Tablet, creating the most robust, feature-rich tablet platform in the industry. Our tablet content is unique, proven, and will allow Securus to meet the tablet needs of the DOC today and evolve to meet all future requirements.

Securus is dedicated to meeting the industry's demand for tablets, and supporting the positive attributes that tablets bring to corrections. To exceed our customers’ expectations in a tablet program, Securus has dedicated development resources which create and continually enhance the best software applications, processes, security protocols, and management capabilities in the market. Based on direct conversations with many agencies across the United States, our tablet solutions have “far exceeded” any provider in the industry. This feedback reflects not just our software applications, consumer options, break/fix processes, and support, but also our network architecture designed to keep the program secure and controlled, making sure that inmates do not gain access to unsecured content or websites. Most important, Securus has delivered on all of our promises to those seriously interested in deploying a tablet program. We are confident that our tablets will allow you to do much more with fewer resources by empowering inmates to be more self-sufficient.

Managed Access Solutions (MAS)
Corrections facilities have been struggling with inmates’ increased usage of contraband cell phones within prisons and jails for many years. Contraband cell phones are being
smuggled into prisons in large numbers and continue to pose a threat to public safety. Securus' Managed Access Solutions (MAS) is a solution which allows correctional facility representatives to effectively control contraband cell phones without impacting legitimate wireless communications within the designated areas of a prison or government facility.

Securus’ MAS solution is a combination of a specially managed cellular telephone system network and a tightly controlled Distributed Antenna System (DAS). It is compatible with 2G, 3G, and 4G technologies and protocols used by U.S. wireless cellphone carriers. The solution manages the mobile devices and applies policy rules determined by the corrections administrators.

Our MAS solution provides efficiencies by reducing physical searches for contraband cell phones, expanding investigative capabilities into contraband cell phones, and preventing crimes from being committed or coordinated by use of contraband cell phones. The MAS delivers correctional facilities an automated solution which fully manages all cellular telephone access 24x7x365 days a year with minimal resources, and provides the facilities with full control of the solution, both locally and remotely.

Conclusion
We are fully committed to consulting with the DOC to further understand the department’s goals, requirements, and concerns so that we may tailor our solutions to completely meet your requirements and evolve with those needs. We will do what we say and say what we will do. With ever-shrinking budgets and limited resources, we are the best option to help the DOC achieve its goal of providing a safe, secure, and efficient corrections environment.

Please contact me or your National Sales Manager, Adam Mercer, with any additional questions or to provide any additional information you may need. You can contact Adam by either phone at (904) 613-8477 or by email at amercer@securustechnologies.com.

Thank you again for this opportunity and we look forward to meeting with the DOC to better understand the department's requirements and to present our inmate telephone, tablet, and managed access solutions.

Sincerely,

Robert E. Pickens
President
Securus Technologies, Inc.
14651 Dallas Parkway, Suite 600
Dallas, Texas  75254
BPickens@securustechnologies.com
COMPANY BACKGROUND
Company Background

For almost 30 years, corrections industry constituents - facilities, inmates, and the family and friends of inmates - have relied on Securus Technologies and our predecessor organizations for communication solutions designed to fulfill their specialized needs.

Securus began in 1986 as an inmate telephone service provider. Over the course of nearly 30 years, we grew to serve over 3,450 correctional facilities and agencies throughout the United States.

In 2009, Securus made a strategic move. Understanding how advanced technologies could radically change the civil and criminal justice industries, Securus executed a plan to leverage our technical expertise and expand our portfolio with complementary products and services that go beyond traditional inmate telephone communications.

Our customer base throughout the nation is growing because we offer compelling products such as our advanced investigative capabilities, tablets and other inmate self-service products and features. We continue to expand our reach while remaining focused on the civil and criminal justice industry.

While we are proud of our heritage, we have not rested on our accomplishments. We continue to re-invest in our people, platforms, and products and have committed over $22 million in incremental spending over the last year to further our industry leading capabilities.

With nearly 200 technology patents today and many more pending, Securus is the clear intellectual property holder for the industry. Innovation is standard at Securus we are without a doubt the leading technology innovator in our industry. Our patents and intellectual property represent more than three times the rest of the industry combined.

Securus products and services are designed to evolve with the market to ensure our customers are able to provide their constituents with the safest environment possible, and to provide your officers with ways to increase efficiency through system interoperability. No competitor can match our level of re-investment or our commitment to solving customer issues. We are committed to continuing to lead our industry and be the best partner we can for our clients.

SECURUS
AT A GLANCE

- Nearly 3,500 agencies and correctional facilities
- 1.2 MILLION inmate calls connected every day
- 99.9% network uptime
- Almost 240 patents issued and pending
- More than 1,000 employees
- 98%+ customer retention rate
- $200,000,000 average investment in new technology each year
Client Focus

Securus provides technology services to hundreds of State Departments of Corrections, County and private prison facilities that house thousands of inmates. We are currently providing our solutions to many of the largest State Departments of Corrections in the Country to include the States of Pennsylvania, Florida, Louisiana, Connecticut, Arkansas and many more. Additionally, through our fully owned subsidiaries JPay and Satellite Tracking of People (STOP) there are few State DOCs that are not utilizing a Securus owned solution to include the Commonwealth of Virginia Department of Corrections.

Securus SCP Inmate Telephone platform is the most utilized Inmate Telecommunications platform in the industry providing more information sharing opportunities than any other provider. This has expanded not only your ability to provide outstanding communication services to your constituents, but also the opportunity to foster interagency cooperation to enhance investigations.

We retain over 95% of our customer base each year which drives us to work hard every day to meet our customers evolving needs. We do this by providing quality, consistent systems that produce real results and service with quarterly upgrades at no cost to our customers; preventing our platforms from becoming obsolete and allowing greater use of technology to benefit facility operations.

The work Securus Technologies does is rooted in deep beliefs:

- The work of public safety, law enforcement and corrections officials matters
- Technology must never get old
- Better communication results in better operations and lower recidivism
- There is no shortage of data, only difficulty in knowing what pieces of data need attention
- Accountability matters, so service and innovation should never be outsourced

We understand that customers have a choice of providers. We've always been a partner that provides high quality products and services at a fair price. We focus on delivering excellence with the ultimate desire to gain total customer satisfaction, confidence, and loyalty.

We value teamwork, partnering and building effective and healthy long-term relationships with fellow associates, customers, suppliers, and other organizations with whom we interface.

We seek to be recognized as a technological leader in our industry and thus are committed to developing products, systems, and equipment that meet customer needs now and in the future.
Financial Stability

Securus possesses the strongest financial position industry. We have an “A” rating with the Better Business Bureau and we’re a stable solid, secure organization who maintains full ownership of our platforms, application, and service capabilities. We continue to grow as an organization, which allows us to continue to fund growth in innovation for our customers.

Organic Growth

Over the last ten years Securus has grown significantly. Securus has grown through customer retention and new customer acquisition, while the only other growing company in the inmate communications market has primarily grown by acquiring other companies to get their customer bases. Securus has been active in acquiring companies over the last several years as well; none of which are inmate calling companies. Our growth has focused on offering a wider suite of products, like our Managed Access and Inmate Tablets to help our customers meet the ever changing landscape. Our portfolio of services is the broadest...
of any Inmate Communications provider and includes the following corrections based solutions.

PUBLIC SAFETY SOLUTIONS
✓ Emergency Response: computer-aided 911
✓ Incident Management: mobile ticketing and reporting
✓ Records Management: automated public inmate info

INVESTIGATIVE SOLUTIONS
✓ Investigation: Threads offers big data analysis with location based services
✓ Verification: JLG Investigator for voice identification and voice biometrics

CORRECTIONS SOLUTIONS
✓ Communication: telephone service, instant mail, video visitation, voice mail, video mail
✓ Information Management: electronic records management, jail management systems, and automated inmate information
✓ Inmate Self-service: kiosk driven inmate applications, inmate tablet media services
✓ Ancillary Services: electronic funds transfer and PREA compliance

MONITORING SOLUTIONS
✓ GPS Ankle monitor: STOP BLUtag, BLUband, BLU+ electronic monitoring of un-incarcerated
✓ Court Monitoring Center: court appointed offender programs
✓ Day Reporting Center: post incarceration court appointed inmate program
Regulatory and Compliance Focus

Securus takes great pride in ensuring our customers are dealt with ethically, and informatively. Securus’ employs a dedicated regulatory team to ensure compliance with all FCC and other national and state regulatory agencies and as part of our agreement will provide regular updates to the VA DOC on these matters. Unlike others, Securus doesn’t subcontract this responsibility to an outside agency and our Legal and Regulatory team consists of all full time Securus associates. Securus routinely goes above and beyond in its ability to provide an environment of compliance and integrity to provide our customers services without concern over poor press due to unfair rates and charges.

For example, unlike our competitors that do not provide transparency or vigor in their financial reporting, Securus is proud to be the only inmate telecommunications provider in the U.S. that is Sarbanes-Oxley Section 404 compliant. This means an independent accounting and auditing firm completed a comprehensive and in-depth evaluation and testing of Securus’ internal controls over financial reporting reinforcing that our financial statements provide the necessary depth and accuracy required for investors, rating agencies and our correctional facilities customers.

Securus can also claim the distinction of being SAS-70 Type II certified. In 2009, Securus successfully completed an American Institute of Certified Public Accountants Statement on Auditing Standards No. 70 (SAS 70) certification, now known as SOC-1.

A SOC-1 certification indicates that an independent accounting and auditing firm completed a comprehensive and in-depth evaluation and testing of Securus’ internal controls and related activities. This certification confirms that the company has effective controls and safeguards in place to manage information and data belonging to its customers. We take this valuable extra step to ensure our customers benefit from the high level of transparency and integrity that Securus provides over other vendors.
INMATE TELEPHONE SYSTEM OVERVIEW
Secure Call Platform Overview

The Securus Secure Call Platform (SCP) is a state-of-the-art, web-based system designed to provide the DOC with the ultimate in inmate call control and reporting. SCP’s advanced features provide extremely powerful and flexible tools for controlling inmate calling, reducing fraud, increasing investigative capabilities, and generating valuable administrative reports. The system is designed to adapt to your facilities and operations, rather than requiring you to conform to the software. To go further, our systems are available over multiple hardware configurations furthering the flexibility we have in system deployment.

The Securus development team custom-built SCP for the corrections industry, making this platform a fully-integrated system of simple-to-use software tools, and computer and telephony hardware. SCP’s hardware and software components readily adapt to the changing needs of a facility’s operations. SCP can monitor, record, and block/unblock inmate telephone calls, and generate reports in real time.

With software updates provided three to four times per year, SCP will keep the DOC on the cutting edge of technology without any additional cost for system upgrades. Because SCP operates on a centralized platform, Securus can customize our solution to your specific needs, addressing the specific operating requirements of your department both today and well into the future.

SCP will support the DOC in safeguarding the community through proactive fraud prevention and advanced investigative capabilities. SCP allows our customers to operate a smarter and more efficient jail through system interoperability while providing the flexibility to interface with your current operations. SCP’s investigative tools permit a higher degree of accuracy and allow investigators to locate inmate-calling information more quickly and reliably. The system is scalable and flexible, reducing labor demands by automating many tasks. Routine inmate calling operations can be configured to require minimal administration, allowing your staff to focus on what they do best—maintaining a safer, more secure correctional environment.

SCP also increases usability by providing anywhere, anytime access for authorized personnel. All of the investigative and administrative resources are available to approved personnel through our secure single-point of access, the SCP user interface. Users can access SCP any time from any Windows-based computer with access to the Internet allowing your investigators to follow the leads wherever they may go.
Secure Call Platform Features

The Securus SCP gives the DOC control over most system features. That means you have complete control to customize the system to your specific needs, even as those needs change. We are committed to using technology to help you safeguard the public and solve and prevent crimes.

Key features include:

- Centralized architecture
- Anytime/anywhere system access using an Internet-enabled computer from any location
- Real-time software/system upgrades three to four times per year at no cost to the DOC
- Premium digital quality superior to that of analog-based systems, which is especially important for investigative purposes
- Remote monitoring 24x7x365 from Securus' Network Operations Center—we monitor system performance and can recognize and correct problems before you are aware of them.
- Advanced call recording management through a patent-pending technology to safeguard the chain of evidence controls on each recording, backed by free, professional testimony
- User-friendly reporting and self-help capabilities
- Information-sharing among partner agencies

Investigative Tools

- Monitoring and recording available on all calls (other than those marked as ‘private’)
- Patented three-way call detection and prevention
- Patented remote call forwarding detection
- Patented Perma-Block allows called parties to block future calls from the facility
- Covert Alert with Barge-In
- CrimeTip hotline
• Scan Patrol
• Case tracking (call notes)
• Investigative reports, such as frequently called numbers, pattern dialing reports, and more
• THREADS call analytics – the ONLY big data analytics solution designed and developed exclusively for corrections and law enforcement
• Location Based Services to identify the location of any call placed to a cell phone from the system
• Proven Voice biometrics, including Continuous Voice Verification
• ICER identifies inmate-to-inmate communication within the DOC as well as with other agencies
• Reverse Lookup with mapping
• Word Spotting

Fraud Controls

• Patented three-way call detection and prevention
• Patented remote call forwarding detection
• Dual tone multi-frequency (DTMF) detection to prevent:
  o Secondary dialing
  o Switch hook dialing
  o Black boxing
  o Hacking
• Velocity restrictions
Service Features

- 24x7x365 Network Operations Center monitoring
  - You operate around the clock, and so does Securus. We can find and fix most problems before you are aware of them and we are here to help you with your questions and requirements whenever you need us.

- 24x7x365 Technical Support through Securus’ in-house Technical Support Center
  - We have the largest employee base in the industry to serve you better and to make sure we continue to lead with enhanced technology.

- 24x7x365 end-user support through our in-house Securus Correctional Billing Services
  - Securus is unique among national competitors in that we operate our call center. We do not outsource our customer experience. We find our end-user satisfaction ratings improve 22% when they use our call center. Providing good service to your constituents cuts down on complaints and provides a better experience for all. We are available to serve callers 24 hours a day.

- Ongoing training as well as training for each new software release (typically provided three to four times per year)

Call Completion

- More billing agreements with local exchange carriers than any other inmate phone provider
- Convenient points of sale and cost-effective terms for prepaid friends and family accounts
- Numerous funding options
- In-house Securus Correctional Billing Services customer service center
- Lobby Kiosks
- Website funding
- Western Union funding
- MoneyGram funding
- Collect, prepaid collect (AdvanceConnect), prepaid calling cards, and debit options
- Inmate PINs
- Inmate PANs – allowed number lists
  - Like all other features of SCP, the PAN lists are flexible and may be administered in various ways: PANs can be configured manually, automatically, or by importing through integration.
- Patented Automated Operator Services (AOS)
- Customizable call prompts, branding, and overlays
- Multi-lingual call prompts
- Inmate name recording

**Administrative Features**

- Audit and activity tracking of system users
- Multi-level password controls
- Access control by day/time, as well as by IP address if desired
- Easy auditing of investigative time spent listening to inmate call recordings

**Call Controls**

- Global blocked number lists
- Global allowed number lists
- Calling restrictions, including duration and velocity by inmate, dialed telephone number, inmate phone, phone group, customer, or facility
- Automatic or manual system on/off controls
- Emergency Call
- Automatic management of calling restrictions
Automated Operator Services

SCP includes an Interactive Voice Response (IVR) system that provides Automated Operator Services (AOS). This automated assistance uses clear and concise, professionally recorded voice prompts to establish call acceptance and to assist inmates and called parties throughout the calling process.

When the called party answers the phone, SCP’s advanced answer detection triggers the call acceptance voice prompt. The called party hears, “Hello, you are receiving a collect call from [inmate’s name], an inmate at the VA DOC. This call is subject to monitoring and recording.” SCP then gives the called party the following menu options:

- “To accept this call, press 1.”
- “To refuse this call press 2.”
- “To hear the rates and charges for this call, press 7.”
- “To block future calls to your number, press 6.”

Additional options provided by AOS include:

### Available Options to Called Parties

- Request a rate quote
- Hear the name of the facility and inmate calling
- Accept or reject the call
- Request available balance of an AdvanceConnect account or available credit of the Direct Bill account
- Hear instructions on how to add more money to their prepaid account or pay their Direct Bill Account
- Connect to a live agent to setup a pre-paid account
- Choose to hear the prompts on the system in English, or the language selected by the inmate (if configured for this option)
- Pay for the incoming call with InstantPay (if available)
- Hear optional marketing message (by request of the DOC)
- Block their number prior to accepting a call using SCP’s patented Perma Block technology*

### Available Options to Inmates

- Listen to prerecorded announcements
- Choose to place a collect or debit call; if debit, PIN entry is requested, the inmate hears the available balance in their account and the cost of the call
- Select a specific language at the beginning of the call (if configured)
- Acknowledge that the call is going to be monitored and recorded
- Hear available call time (prompt will tell the inmate call time limits based on calling schedules or calling restrictions)
- Identify themselves by PIN or Voice Biometrics (if configured)
- Add, remove, and/or listen to the phone numbers on their PAN list (if configured)
- Hear optional marketing message (by request of the DOC)
Bilingual Capability

The Securus SCP default system setup provides message prompts in both English and Spanish. Inmates select a specific language at the beginning of the call process by dialing a single digit.

During call acceptance, the called party receives the acceptance instructions in English first and then receives an option to continue in the language the inmate selected. This fraud deterrent feature eliminates possible attempts by the inmate to confuse the called party with a language they do not understand.

Securus provides durable printed dialing instructions in both English and Spanish on each inmate telephone, using materials and techniques appropriate for the correctional environment that explain the process in a clear, easy to read manner:

Sample Dialing Instructions in English and Spanish

<table>
<thead>
<tr>
<th>DIALING INSTRUCTIONS</th>
<th>INSTRUCCIONES PARA LLAMADA</th>
</tr>
</thead>
<tbody>
<tr>
<td>This Call is Being Recorded</td>
<td>Esta Llamada va Hacer Gravada</td>
</tr>
<tr>
<td><strong>Press '1' for English</strong></td>
<td><strong>Marque '2' para español</strong></td>
</tr>
<tr>
<td>For a collect call, press '1'</td>
<td>Para llamada a cobrar, marque '1'</td>
</tr>
<tr>
<td>For a debit call, press '2'</td>
<td><strong>Para llamada de débito, marque '2'</strong></td>
</tr>
<tr>
<td><strong>TIPS Hotline, press '8'</strong></td>
<td><strong>Para línea de aviso secreto, marque '8'</strong></td>
</tr>
<tr>
<td>Enter your PIN number</td>
<td>Marque su número de identificación personal</td>
</tr>
<tr>
<td>Enter your area code and phone number</td>
<td>Marque su número de teléfono, incluya su código local o lada</td>
</tr>
<tr>
<td>You may hear silence during the acceptance of your call. Please continue to hold.</td>
<td>Vas a oír silencio mientras aceptan su llamada. Continue esperando por favor</td>
</tr>
</tbody>
</table>
Multilingual Language Prompts

The Securus automated operator uses clear, concise, professionally recorded voice prompts to assist the inmate through the calling process. By default, the Securus Secure Call Platform (SCP) offers language prompts in both English and Spanish. Securus can provide additional languages on request. SCP can be configured to provide prompts in as many as nine languages.

Some examples of languages that Securus has implemented in the past include:

- Afrikaans
- Arabic
- Bahasa
- Bulgarian
- Chinese (all dialects)
- Creole/Haitian
- Croatian
- Czech
- Danish
- Dutch
- Estonian
- Finnish
- Flemish
- French (Canadian and Parisian dialects)
- German/Bavarian
- Greek
- Gujarati
- Hebrew
- Hindi
- Hungarian
- Icelandic
- Italian
- Japanese
- Javanese
- Kannada
- Korean
- Latvian
- Lithuanian
- Malay/Malayalam
- Marathi
- Norwegian
- Polish
- Punjabi
- Romanian
- Russian
- Slovak
- Slovene
- Somali
- Spanish (U.S., Mexico, Puerto Rico, Central and South America, Castilian dialects)
- Swedish
- Tagalog
- Taiwanese
- Tamil
- Telugu
- Portuguese (Brazil and Portugal dialects)
- Thai
- Turkish
- Urdu
- Ukranian
- Vietnamese

After the language prompts are set up in the SCP system, inmates select their language choice at the beginning of the call process by dialing a single digit.

During call acceptance, the called party receives the acceptance instructions in English first followed by an option to continue in the language selected by the inmate. This fraud deterrent feature eliminates inmate attempts to confuse called parties with a language they do not understand.
Securus will also provide durable printed dialing instructions at each inmate telephone location in English, Spanish, and the other languages specified by the DOC. As a security measure, Securus will use materials and techniques appropriate for the corrections environment that explains the process in a clearly defined and easy to read manner.

Commissary Order by Phone

The Securus Commissary Order by Phone product allows inmates to order commissary items using the same inmate telephones they use to place calls to friends and family members.

Benefits for Your Facility

This product saves facility staff the time processing commissary orders and handling order complaints. Commissary Order by Phone frees your staff to focus on important activities like safety and security. Your facility will see an increase in sales of commissary items by offering an additional point of sale increasing commissionable revenue.

Benefits for Inmates

Inmates can place orders when and as frequently as needed, using Commissary Order by Phone. The ordering process is convenient, easy, and accessible and does not require facility staff. To place an order, inmates go to any inmate telephone and dial a designated number. The call then connects to the commissary’s IVR where the inmate places their order by following the voice prompts and pressing keys on the phone keypad.

Benefits for Commissaries

Commissaries also benefit from Commissary Order by Phone. Another point-of-sale increases commissary revenue and improved inventory turn times.
On/Off Station Control

The Securus Secure Call Platform (SCP) provides complete flexibility to disable telephone use at any time of day through manual intervention or preset calling schedules.

SCP allows authorized users to disable a telephone, group of telephones, or all facility phones using any personal computer with access to the Internet. Securus is one of the only providers to offer this capability anytime, from anywhere, 24 hours a day, seven days a week. This function allows authorized users to either kill the call immediately or allow current calls to finish while not allowing any new calls.

Disabling Telephones

Disabling Telephones

Authorized users enable or disable phones from anytime, anywhere.
PIN Operation (Open & Controlled)

With the Securus Secure Call Platform (SCP), each inmate telephone is individually programmed for Personal Identification Number (PIN) or non-PIN operation. This provides maximum flexibility in PIN placements. For example, a facility may wish to allow PIN operation in maximum security or long-term areas, while allowing an “all calls” option in overnight, work release, or trustee areas. SCP has no limit or restrictions on the number of PIN or non-PIN inmate telephones operating at the facility.

Some facilities may choose to assign each inmate a unique PIN that they must enter before making a telephone call. PINs also provide an audit trail of the inmate who placed each specific call. Additionally, PINs allow the facility increased control over which inmates can call which numbers.

Each inmate is assigned a unique PIN, ranging anywhere from 4 to 16 digits. This range creates a maximum number of 9 billion PIN combinations.

Facilities can choose one of the following three primary modes to a single phone or group of phones in a facility:

- Mode 1, Open PIN
- Mode 1, Open PIN with Restrictions
- Mode 3, Closed PIN

Mode 1, Open PIN

This is the most basic mode of operations, and the simplest to administer. Each inmate is assigned a unique PIN to make a phone call. There are no individual phone number restrictions or calling lists in this mode. SCP applies global system calling restrictions to every call.

Mode 2, Open PIN with Restrictions

Mode 2 builds on the Mode 1 Open PIN feature and adds the ability to place call restrictions and limits on specific call types while allowing all other phone numbers to process as they would in an Open PIN system. Mode 2 restrictions can include the recording and alarming of numbers and the use of the facility or global number lists for special circumstance numbers, such as attorneys and external crime tip numbers.
Mode 3, Closed PIN

Mode 3 provides the most restrictive calling privileges. It also requires the most administration of the three modes. Each inmate registers telephone numbers on their calling list. The total number of destination numbers available is unlimited. The facility determines the maximum number of telephone numbers each inmate can register. Telephone number registration includes the number, name of the called party, and their relationship to the inmate. The telephone numbers that each inmate registers are associated with the inmate’s PIN and reside in the system. Only that PIN may validate calls to those numbers. Updating calling lists is a continuous process as inmates are booked into, or released from the facility, or as the inmates request changes to their calling lists. This type of control is usually recommended only for facilities with a low rate of inmate population turnover, or where such extreme security measures are desirable. Note that in a Closed PIN environment, the facility may choose to make certain telephone numbers commonly available to all inmates. The common numbers may be assigned global or facility accounts.

The system can set a maximum time limit for any call or all calls from an individual PIN or all PINs. Administrators can tie many additional restrictions to any PIN or telephone, or telephone number associated with a PIN such as:

- Time of day and/or day of week
- Maximum duration of a call for that PIN or phone
- Maximum number of calls or minutes an inmate may use per day, week, or month

The calling platform automatically manages all imposed calling restrictions.

Securus provides an automated PIN and PAN management system called E-Imports that can off-load facility labor required to enter PINs and PANs manually.
Personal Allowed Number List

The Personal Allowed Number (PAN) feature in the SCP provides an approved calling list for each inmate. The PAN restricts inmate calling to only those numbers on their list.

Securus built this feature with the awareness that each facility has unique needs for implementing allowed calling lists. Like all other features of SCP, the PAN lists can be administered manually, automatically, or by importing through E-Imports. The PAN configuration options include:

- **Auto Pan.** Allows the first “X” numbers (defined by the DOC) to be added to the inmate's PAN list automatically. The quantity of numbers allowed is configurable. This is the most popular method of PAN administration. Numbers are loaded immediately without the intervention of staff, maximizing revenue potential.

- **Inmate Managed PAN.** Allows inmates to manage phone numbers on their list such as adding a new number, removing a number, checking the status of a phone number, or hearing the phone numbers are on their list. When an inmate adds a phone number to their list, the automated system conducts a real time Billing Name and Address (BNA) lookup on the phone number. If SCP finds a valid BNA, it will call the phone number and ask the called party accept being on the specific inmate's PAN list. No staff time is required to administer this process. With the extra step of validation, the DOC has maximum control of each added number.

- **Manual PAN Entry.** Authorized facility personnel have the ability to accept calling lists from inmates, verify the phone numbers, and enter them into the SCP user interface. This form of PAN administration allows a hands-on approach to approval and control of each number added to an inmate’s allowed number list.

- **PANs by System Integration.** SCP allows for the importing of Personal Allowed Numbers through our E-Imports application to add, create relationships, and deactivate numbers. No staff time would be required to administer this process. This is a specialized form of PAN administration, based on specific integration requirements of a facility.

**Additional PAN Features**

The SCP provides administrators additional features to maximize efficiency, control, and inspection of PAN lists:

- **Global Allowed List**
The following table provides descriptions of each PAN features and their primary benefit to the DOC.

<table>
<thead>
<tr>
<th>PAN Feature</th>
<th>Primary Benefit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Allowed List</td>
<td>Efficiency</td>
<td>Certain phone numbers, such as attorney numbers, can be authorized for all inmates by including them on SCP’s “global allowed list.”</td>
</tr>
<tr>
<td>Automated List Refresh</td>
<td>Efficiency</td>
<td>With this automated feature, PAN lists can be configured to refresh every month on a certain day, such as the first of every month.</td>
</tr>
<tr>
<td>Verified/Not Verified PAN</td>
<td>Safety and control</td>
<td>This feature flags numbers added to the inmate's PAN list as “verified” or “not verified.” If the PAN is “not verified”, the inmate can call the number for a configurable number of days before it is blocked. Once the threshold number is reached and the number is blocked, a facility administrator must verify the number and if appropriate, allow calls to that number again.</td>
</tr>
<tr>
<td>Speed Dial for PANs</td>
<td>Safety and control</td>
<td>Setting up speed dial numbers for PANs is a preventative measure that reduces an inmate's ability to steal or use other PINs or PANs.</td>
</tr>
<tr>
<td>Associate PANs to PINs</td>
<td>Safety and control</td>
<td>SCP associate PANs with specific PINs. Administrators can apply restrictions to PINs giving facilities control over when and where an inmate can place a call, how long they can talk per call, and how many calls they can make by day, week, or month.</td>
</tr>
<tr>
<td>PAN Management Report</td>
<td>Efficiency</td>
<td>This user-friendly, interactive report provides a dashboard view of all PAN entries in the system. The report indicates PAN</td>
</tr>
<tr>
<td></td>
<td>entries entered into the Inmate Managed PAN System. Users can select from more than twenty criteria to produce reports with multiple data points. All reports are exportable to Excel, CSV, and PDF.</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td><strong>PAN Change Log Report</strong></td>
<td>Safety and control</td>
<td>PAN Change Log functionality records all actions that SCP users make to the verified field in the SCP user interface. It also allows administrators to examine all PAN list changes; specifically, when changes occur, and by whom, helping administrators and investigators track user accountability.</td>
</tr>
<tr>
<td><strong>PAN Frequency Report</strong></td>
<td>Safety and control</td>
<td>Shows phone numbers that appear in multiple PAN lists. Users have the ability to enter threshold numbers to define search criteria. For example, a threshold of “four” will show phone numbers that appear in PAN lists more than four times. This report also allows users to create a detail report with specific detail for each call.</td>
</tr>
</tbody>
</table>

**Simultaneous Recording and Monitoring**

The Securus Secure Call Platform (SCP) has an integrated recording and monitoring system. The automated system is designed to be a cost-effective solution for all correctional facilities of any size. Multiple levels of security provide that only authorized personnel can access and monitor the inmate recordings and that only non-privileged calls are recorded. Authorized personnel can listen to live or archived recordings via multi-media PC interfaces connected over local area networks (LANs).

**Call Monitoring**

The SCP Live application allows for real-time monitoring of calls in progress via a multi-media PC workstation. Facility personnel (with appropriate privileges) can monitor live calls by highlighting the call in progress and clicking on the speaker icon. This process is undetectable by the inmate or the called party and does not disrupt the recording process. Concise descriptions of activity appear for each phone in use. For example, the system shows the specific telephone location, inmate PIN, the destination number dialed, city and state of the destination, and start time and duration of each call. SCP also displays any
restrictions such as “watched” or “private,” and the status of the call, such as “in progress,” “calling destination,” or “getting acceptance.”

SCP can also automatically eliminate all monitoring or recording of special calls, such as calls to legal counsel, by designating the number as a “private” number. SCP prevents all unauthorized attempts to listen to private calls—the user interface will not display the speaker icon to play private calls. The call record also lists the call as “private” on the user interface.

Call Monitoring, Silent

When monitoring occurs, the system incorporates analog suppression/amplification hardware that allows monitoring of calls without inmate or called party detection. There is absolutely no noise, volume loss, or other indication of monitoring to assure complete investigator anonymity.

Call Recording

The integrated SCP recording application works independently, so there is never a need for integration of a third-party manufacturer’s product. This allows the facility to deal with a single vendor if any issues arise.

The SCP uses large capacity hard drives, along with RAID (Redundant Array of Independent Disks), that virtually extend the call storage period to meet your specific needs. Recordings are stored on-line for immediate access for 12 months. The SCP can also burn the information to CD or DVD for additional back up, if necessary.

The SCP can record all calls simultaneously and allows personnel to listen to pre-recorded calls while active calls continue to be recorded. The system records the entire conversation from call acceptance to termination.

Remote Access to Recording and Monitoring

With integrated recording and monitoring applications, other agencies, such as the local police departments, can also access these functions. Any authorized user with an approved user name and password can easily, and remotely, access recording and monitoring of inmate calls from any computer or device with access.
to the Internet. Securus has tested and certified the playback of calls and live monitoring on:

- Operating Systems/Devices
  - iOS
  - Android OS
  - OS X
  - Windows

- Browsers
  - Internet Explorer
  - Firefox
  - Chrome

Recording Search and Retrieval

Securus allows access from facilities and investigators to research calls via SCP’s user interface. The SCP user interface provides single-point access to all the investigative tools provided on the platform.

Investigators can specify search criteria for calls, such as called party, calling telephone, date, time, PIN, account, duration, and locations then search across a site or group of sites based on their security authorization. SCP searches call detail records and can include all call attempts or just completed calls.

Search results allow for viewing of detailed information about the call and whether or not it was recording. If recorded, authorized investigators can listen to the recording using a powerful call player with easy-to-use search capabilities, and features such as, pause and play.

To speed searching of a recording the player shows sound wave activity of the call to identify times of limited talk or to identify a particular event.

SCP streams call recordings to a program on an investigator’s computer that can ‘play” the recording through the attached speakers. Chain of Evidence safeguards are in place to prevent access to the actual digital copy of the recording and to eliminate any chance of manipulation, whether intentional or accidental, that could later challenge the authenticity of the call recording.
Call Recording Storage

Securus facilitates anywhere, anytime, immediate access to stored recordings online for the contractually-required length of time. Securus stores call recordings in centralized, disaster-resistant, carrier-class data centers. All equipment used to store recordings is monitored by the Securus Network Operations Center (NOC) 24 hours a day, seven days a week, and 365 days a year.

For redundancy, SCP writes all recorded calls to two separate Storage Area Networks (SANs), using two separate connections. Securus also archives all call recordings to an offsite storage facility for the third layer of redundancy. Recordings can be downloaded from SCP in various, widely-used formats and copied to a CD, DVD or any drive (such as a removable flash drive).

The Securus SCP provides a unique set of features and advanced technologies to store call recordings. Traditional premises-based calling platforms use local hard drives that may fail and are susceptible to local disasters. Premise-based systems needed manual backup schemes that are no longer necessary with SCP. SCP uses Storage Area Networks (SANs), special-purpose, high-speed networks that interconnect different kinds of mass storage and shared storage devices (such as disk arrays, tape libraries, and optical jukeboxes) with associated data servers.

The SAN architecture makes all storage devices available to all servers on the network. The SAN solution delivers complete scalability for a facility’s storage requirements and supports disk mirroring, backup and restore, archival and retrieval, data migration from one storage device to another and the sharing of data among different servers in a network.

New storage devices added to a SAN become accessible from any server in the network. The SAN uses a series of standards to spread data across multiple drives for additional protection and redundancy. This technology enables the SAN to deliver superior performance and fault tolerance to disk failures ensuring data is no longer susceptible to drive failures. Accordingly, the SAN provides facilities with the ultimate protection against drive or server failures.

Within the SAN, SCP utilizes a combination of several RAID technologies including RAID5, RAID6, and RAID10. Even if one of the hard disk drive fails during the data recovery process, the system will continue to operate without data loss.
The Securus SAN has more than four (4) petabytes of storage space and is continuously monitored and managed through automated processes and storage policies. When these very large storage systems approach designated thresholds, Securus expands capacity to ensure all authorized call records and recordings are retained in secure, disaster-resistant locations.

The Securus data center storage solutions provide facilities with technology that is:

- **Scalable** to meet any facility’s contractually required storage demands
- **Resistant** to local disasters through multiple copies stored within the data centers and off-site
- **Highly available** through the unique architecture and design of the data storage model
- **Partitioned** and **compressed** to run queries faster
- **Secure, protected, and monitored** to enable total recall of data

SCP records and stores basic call data with the capability to provide management reports. Securus does not limit the call data storage time. Since every site’s requirements are different, Securus works with each facility customer to define their optimal data storage timeframe. All recordings are stored online as well as on remote copies. Typically, call detail records are stored for seven years.
Call Tracker

The Securus Secure Calling Platform (SCP) allows authorized users to add notes and tracking numbers to call detail records associated with recordings. Using this feature, known as Call Tracker, users click the notepad icon located in the call detail record, to add notes to an inmate call. The Call Tracker feature gives authorized users the ability to add a tracking number, gang affiliation, duration into the call, and any other notes associated with the call. This feature also allows authorized users to either keep the note private to their investigation or to share the note with other users. From the Notes screen, users may also view previous notes associated with the same call.

Adding a Note to a Call Detail Record

Click the “notes” icon to add a note to any selected call detail record.
When searching for Call Tracker entries, users can navigate to the Call Tracker Search Tool. The Search Tool allows users to search entries by tracking number, authorized user name, phone number dialed, inmate account number, and PIN. Users can also complete a full-text search on the notes added to the call, such as gang affiliation and the start or end date of a call. As with every report in the SCP user interface, the search results are exportable to Excel, PDF, or CSV.
Extending Expiration Dates

SCP's Call Tracker feature can extend the expiration of a recording. At times, investigators do not want recordings from active investigations purged from the system—regardless of the recording retention policy in effect. Authorized users can protect a recording from being purged by extending the expiration of the call by 30, 60, 90 days, or for the life of the contract by selecting the Extend Expiration icon.

Extending Call Recordings
When downloading calls from the SCP user interface, users add calls to a Recording Management folder. This folder allows users to add multiple recordings to a folder for ease of management. When a Recording Folder is downloaded, any associated Call Tracker entries can also be exported through Call Tracker to the downloaded recording folder.

Managing Recordings

Securus allows investigators to access all investigative tools via a single web portal known as the SCP user interface.

Investigators can search for calls using criteria such as called party, calling phone, date, time, PIN, account, duration, and locations. Search can be across a single site or group of sites based on their security authorization. Searches can include all call attempts or just completed calls. The searched results provide detailed information about the call indicating the presence of a recording.

Investigators can listen to recordings, within the limits of their security access, using SCP’s powerful call player. The player includes easy-to-use search capabilities, and features such as pause and fast-forward. A visual waveform helps investigators bypass areas of limited talk time and to quickly identify particular events.
When listening to a recording, the audio is “streamed” to the user’s computer. This safeguards the original recording. Chain of Evidence safeguards prevent access to the original recording to eliminate any chance of intentional or accidental manipulation or deletion.

Calls within the contractual storage period can be retrieved within the requested timeframe. Call recordings that are marked store for life of contract could take slightly longer to retrieve because of the required data mining.

Software Upgrades

We recognize that the challenges you and your officers face every day never stop evolving. When designed our centralized platform, one of our chief objectives was deploying a system that provided upgrades to all customers at regular intervals with no downtime. We achieved that objective with SCP. Securus provides upgrades to all of our customers three to four times annually through a proven and tested after hours process that allows all sites to immediately realize the benefits each upgrade. Our system delivers proven features driven by input from the most recognized corrections and law enforcement agencies in the nation.

Maintenance events are always preceded by a splash screen displayed at login notifying the facility of the upcoming upgrade and new features are discussed with customers prior to implementation. These system updates are more than simple changes. They provide meaningful features and new capabilities, which drive greater officer and community safety, staff efficiency and improved investigative response times.
The following image shows the sample splash screen that notifies users of upcoming maintenance.

Splash Screen

![Splash Screen]

Running SCP Reports

The Securus Secure Call Platform (SCP) retains call detail records on all call attempts. Authorized users can quickly run reports to spot calling trends, assess monitoring efforts, investigate suspicious activities, and manage phone usage.

Users can customize reports by changing search criteria such as date, time, call duration, telephone number, originating telephone, destination, inmate ID, termination reason, and much more.

The following steps show the ease of producing valuable, customized reports:

1. Place the cursor over Tools. A drop down menu will appear.
2. Move the cursor over Reports to see a menu of standard reports.
3. Click on the type of report you want. SCP will display the appropriate fields associated with that report.

4. Verify the correct Management Level is displayed or make changes as necessary. (This setting allows you to select the facilities, sites, phone groups, or phones you want to search.)

5. Enter your search criteria in the appropriate fields and click Search.

The records matching the search criteria will display. With a single click, the data can be instantly exported to Excel, CSV (Comma Separated Values), or Adobe PDF format.

Users will be able to sort on any of the following data elements.

- Site
- Phone Location
- Country Code
- Dialed Number
- Start Date/Time
- End Date/Time
- Duration
- Account #
- PIN
- Continuous Voice Verification
- Agency Type
- Call Type
- Call Status
- Termination Category
- Block Reason
- Privacy
- Watched
- International
- 3-way Detected
- Remote Call Forward Detected
- Promotional Call
- Text Call
- Language
- DTMF Detection
- DTMF Digits
- Text2Connect Call
- Prepaid
- First Name
- Promotional Call
- Voice Biometrics
- Amount
The resulting report can easily be saved, printed out, or emailed to others.

Selecting a Report to Run
Standard Reports Available through SCP User Interface

The Securus Secure Call Platform (SCP) has a dedicated report writer that provides investigative information based on the call detail records. This sophisticated reporting tool provides a reporting interface into all calling activities.

Users can search and analyze call details on all calls placed from each inmate telephone through SCP. These details include date, time, duration, telephone number, origination, destination, inmate ID, termination reason, and more. SCP retains call details on all call attempts. Users can customize the standard reports by varying search criteria, such as date range, facility, or call length.

SCP provides standard reports with parameter fields that allow the user to define the information content of each report based on the following criteria options:

- Per phone, per location, and per offender
- Destination number (partial or full number entry)
- Date and time range
- Call frequency
- Call type (completed, incomplete, blocked)
- Number restriction and/or status assignment
- Personal allowed number cross-referencing
- Graphical display of call fluctuation
- Broad search with no data entry
- Suspected fraudulent call activity
- Offender name
- Offender PIN (if used) and/or account number
- Prepaid calling card number
- Destination zone (local, interLATA, interstate, intraLATA, international)

The Investigative Reports section compiles data and opens the information in a report format, on the workstation monitor. Investigative Reports provides multiple functions for call playback and copying call recordings to remote media. Authorized personnel can use this unique application to generate a report even when only a little information is available.
A full set of reports that administrative users need daily, as well as a full set of investigative reports, makes Securus’ Standard Reports generator anything but standard.

**Call Detail Report**

The Call Detail Report (CDR) provides investigators an intuitive and user-friendly report to view or search virtually anything related to an inmate call, including:

- Site name from which the call originated
- Phone location as labeled in the system
- Facility code
- Dialed number
- Start date/time
- End date/time
- Duration of call
- Inmate Account Number
- Inmate PIN
- Prepaid card number if used
- Inmate first, middle, and last name
- Type of call (voice mail, person call, prepaid call, debit call)
- Status of call (complete/incomplete)
- Reason for call termination
- Reason for block
- Call properties (watched number, RCF detected, three-way attempt, private number)
- Destination zone
- Desired results per page
Call Detail Report

Also, Call Detail Record (CDR) reports allow users to:

- Add notes to a call record or a tracking number
- Mark the notes private or public
- Play the call
- Copy the call to a management folder for download
- Download the call immediately with a one click operation
- Extend the call expiration date if it is approaching the agreed upon storage threshold
- Export the report results (users can export all SCP reports)
- Select a single site, all sites, or allowed sites, and specify information by phone, phone group, or the entire customer profile.
Call Frequency Report

The Frequently Called Number (FCN) feature allows investigators to generate a report by entering a frequency threshold to find only those numbers called more than the specified number of times. Investigators can use this report to determine specific call patterns, detail suspicious activity, and selectively assign a watched number status to potential fraudulent numbers. Search criteria include:

- Threshold (Number of times a phone number was called)
- International
- Watched
- Private
- Termination Category
- Call Type
- Call Status
- Date Range
Call Tracker Report

The Call Tracker Report allows users to track CDR notes (made by themselves or other investigators). Authorized users can export report results to Excel, PDF, and CSV file formats. Search criteria include:

- Not Shared (when checked, shows the user’s notes that are flagged “not share” with others)
- Tracking number
- First and last name
- Custody Account and PIN
- Dialed number
- Notes (allows users to conduct a search using keywords included in the notes)
- Date range
- Results per page
Hourly Usage Report

The Hourly Usage Report shows users the number of phone calls that have taken place within a given date and time range. Users may export the data to Adobe PDF. Search criteria include:

- International
- Watched
- Private
- Call Status (Complete and/or Incomplete Calls)
- Date and Time (Maximum one week search)
Covert Alert Call Detail Record Report

The Covert Alert Call Detail Record Report shows users any Covert Alerts triggered during a specified date and time range. Results can be exported to Excel, PDF and CSV file formats. Search criteria include:

- Alertee Phone Number (The person that the phone call was forwarded to i.e. investigator)
- Alertee first and last name
- Dialed Phone Number
- Custody Account and PIN
- First and last name
- Termination Category
- Call Status
- Date/Time range
Officer Check-In Report

The Officer Check-In Report shows when officers have “checked-in” at different phones and any messages they have left. Users can listen to recorded messages from the report. Results are exportable to Excel, PDF, and CSV file formats. Search criteria include:

- Account number (Of the officer)
- PIN (PIN number associated with an officer)
- Officer ID
- User Name (SCP user ID of the officer if he/she has one)
- First and Last Name
- Call Status
- Date and Time Range
- Results per page
Personal Allowed Number Frequency Report

The Personal Allowed Number (PAN) Frequency Report shows phone numbers that appear in multiple PAN lists. Users enter threshold numbers to define search criteria. For example, a threshold of “four” will show phone numbers that appear on more than four PAN lists.

Personal Allowed Number Frequency Detail Report

The PAN Frequency Detail Report allows users to search PAN lists to see phone numbers that appear more than once.
CrimeTIP Report

The CrimeTIP report allows users to search for and listen to any anonymous crime tip messages left by inmates, outside parties, or officer replies. Search criteria include:

- Mail Box ID
- Call Type
- Date / Time Range
- Results per page
Informant Line Report

The Informant Line Report allows users to search for calls placed to the informant line and distinguish these calls from regular inmate calls. Search criteria include:

- Site name from which the call originated
- Phone location as labeled in the system
- Facility code
- Dialed number
- Start date/time
- End date/time
- Duration of call
- Offender Account Number
- Offender PIN
- Prepaid card number if used
- Offender first, middle, and last name
- Type of call (voice mail, person call, prepaid call, debit call)
- Status of call (complete/incomplete)
- Reason for call termination
- Reason for block
- Call properties (watched number, RCF detected, three-way attempt, private number)
- Destination zone (local, intrastate, interstate, international)
- Desired results per page
Informant Line Report
Secure Call Platform Debit Report

The SCP Debit Report allows users to:

- Query Offender Debit/Prepaid call detail records (CDRs) by user-specified criteria
- View all debits and credits that occurred during a specific period for an individual inmate, for all inmates in a facility, or for all facilities

Secure Call Platform Debit Report

Export capabilities for reports

Authorized users have fast and convenient access to SCP reports. They can save, retrieve, and share reports in the following file formats:

- Adobe® PDF
- Microsoft® Excel
- Comma Separated (CSV)

Users can also save reports to multiple destinations or upload data from the report into their other databases for further analysis.
Disaster Recovery

Securus Technologies has designed and implemented a robust network architecture that provides for quick disaster recovery, minimalizing downtime for the Securus platform and its customers. Securus has demonstrated its ability to recover efficiently under extreme circumstances, restoring service to our customers with no data loss.

Risk Mitigation

Securus has implemented a platform and infrastructure designed to minimize potential outages and protect customer data. Multiple data centers, diverse network paths, redundant platform systems and proactive monitoring mitigate the majority of risks.

Data Centers

Securus maintains a presence in three data centers in three geographically diverse locations. Our data centers are designed to withstand worst case events and maintain 99.95% availability. The data centers, managed and staffed by a carrier-class data center host, meet or exceed the Telecommunications Industry Association’s (TIA) standard number 942 for Tier IV (highest availability) data centers including:

- Ability to withstand a 96-hour power event
- 2-hour fire protection
- Multi-layer physical security
- Multiple power delivery paths.

Additionally, Securus data centers have redundant uninterrupted power systems, N+1 generator redundancy, and N+1 cooling redundancy. All systems and network equipment have redundant power paths. Multiple telecommunications carriers also serve each data center for load balancing and path diversity. Securus data centers are manned 24x7x365 for immediate physical assistance inside the data center.

Multiple checks ensure data center physical security including guarded, photo-verified check-in, dual door authentication (card and biometric), and a mantrap (interlocking door controller) at the data center suite entrance.
Redundancy

Redundancy is a key component of the Secure Call Platform (SCP). While operating on a single platform, Securus' SCP runs on duplicate environments in separate data centers in Atlanta, GA and Dallas, TX. Each component has N+1 redundancy meaning that a failure of any one component does not result in downtime because there is a backup available to resume its function. In addition to the inherent redundancy of SCP, Securus has also designed redundancy into all support systems either through N+1 configuration, database clusters, virtual machines, load balancing or other failover methods. All network transport has redundant network equipment and routing to allow traffic to reroute in the event of a failure.

The SCP platforms in Dallas and Atlanta were designed and built to the same specifications. This standardization allows rehoming of systems from their primary data center to an alternate data center in the event of a failure.

All circuits coming into Securus data centers use multiple diverse carriers, including the interconnections between data centers. In the event of a failure, traffic will reroute across a redundant circuit or path. Additionally, Securus utilizes multiple carriers for inmate calls from the SCP platform. Calls to family and friends will immediately reroute upon failure of any carrier.

Securus utilizes multiple methods of storage to minimize the risk of data loss. All critical systems and data are backed up at regularly scheduled intervals and stored offsite for retrieval if needed. In addition to offsite storage, Securus replicates voice clips, call recordings and validation data between the data centers.

Securus uses industry leading vendors for all platform and network hardware including Dell, Cisco, Oracle, EMC, Big IP and Intel. In addition to the redundancy designed into the platform and network, Securus also maintains a spare parts inventory onsite at each of our data centers to expedite repair of a failed component. Securus also maintains premium-level support contracts with each vendor that defines stringent service level agreements in the event of failure.

Securus maintains an inventory of spare parts for our facility-based components at our headquarters in Dallas, Texas and has distribution agreements with multiple vendors to provide expedited national delivery service. The corporate headquarters maintains a standardized emergency recovery package of frequently used spare parts and equipment that will be available for shipment to support restoral efforts at our customer sites. Our technical field representatives located throughout the country also carries an inventory of the most commonly needed spare parts. With spare parts on board our service vehicles, most facility-based equipment malfunctions can be resolved with a single site visit.
Proactive Monitoring

Data Centers and Network

Securus continuously monitors all data centers, infrastructure components, platform systems and Inmate Telephone Systems (ITS) using the SolarWinds® suite of network performance monitors. The SolarWinds® performance monitors are highly configurable to provide real-time monitoring, event notification, alert history and statistical information. An alarm condition creates immediate visual alerts and email notifications.

The Securus Network Operations Center (NOC) provides 24x7x365 monitoring for all Securus systems, including SCP, network, back-office systems and data centers. The NOC proactively monitors these systems to ensure performance is optimal and uninterrupted. In addition to system and network level monitoring, the NOC also monitors real-time video surveillance and environmental alerts for our data centers. Securus maintains a fully redundant backup NOC at a separate physical location, should services be disrupted at the primary location.

Maximum Number of Inmate Phones

The Securus Secure Call Platform (SCP) is the largest inmate telecommunications platform in the industry, currently supporting more than 2,600 sites and handling approximately 7,000 concurrent calls during peak calling times. The network is engineered to support more than 14,000 concurrent calls. The number of telephones attached to the platform is unlimited, and it is Securus policy to have 30 percent more capacity available than peak volume level. This aggressive network availability policy is designed to ensure inmates can reach their friends and family members at peak calling times during holidays.
Exclusive Investigative Solutions

It is no longer enough just to process phone calls through an inmate telephone system. Inmate calling has become an important part of crime prevention and investigation in every correctional facility. Securus has the largest documented investment in new technology in the industry. We offer the most technologically advanced investigative solutions in the industry as evidenced by our industry-leading patent portfolio.

The Securus Secure Call Platform (SCP) includes more than 500 distinct features; many are specifically designed to identify potential criminal activity conducted through inmate telephones.
Word Spotting

SCP’s Word Spotting is an investigative tool that finds specified keywords and short phrases within inmate conversations. This technology speeds up investigations and reduces labor demands and increases investigative capabilities.

Word Spotting Technology

The Securus Word Spotting solution was developed specifically for the corrections environment. As an experienced innovator, Securus built and tested this technology in our development lab using real calls placed by inmates with feedback and direction from investigators. This approach ensures that the DOC will be using a premier investigative tool with the best accuracy in the industry today.

SCP’s Word Spotting features includes:

- A default dictionary of more than 7,500 search words that can be customized to meet the facility’s needs, including slang and jargon not found in standard dictionaries. As security threat groups expand their code word vocabulary, investigators can add new keywords
- A user-friendly interface to select suspicious inmates or phone numbers for ongoing searches
- A Word Spotting search engine that automatically processes inmates or phone numbers with no additional involvement from facility staff
- Integrated reporting that allows users to identify calls with specified keywords
- A unique feature that allows users to select suspicious recordings from the standard Call Detail Report and send them through the search engine with a single mouse click
Informant Line

The Informant Line provides investigators the ability to set up any phone, voice mailbox or answering machine to answered call from “informants” without any indication in the call detail reports, global lists, or to other inmates. It is a completely anonymous call with all information hidden from normal investigator views.

Informant line setup process

1. User connects to SCP UI with credentials that have access to modify Informant Line calls
2. Navigate to Global List and create a new entry
3. Enter the following information
   a. Dialed Number for informant to call
   b. Select options to show this number, port, speed dial, or inmate account information as “unlisted” in CDR reports
   c. Private if applicable (private calls will not be recorded)
   d. Select the Dialing Class Of Service “Informant Line”
   e. Set the number as “active”
   f. Enter the Speed Dial Code for informant to dial (example: 111)
   g. Set 3-Way Call Detection (Enabled / Disabled)
   h. Enter a Description if desired
   i. Select option to hide phone location in CDR reports
4. Click ‘Create’

Informant line CDR reporting process

The investigator must have security level access to view these calls in a CDR report. A user without access to view “informant line” calls in the CDR report, will simply not see these calls. For those very few users who have this level of access:

Investigator navigates to CDR report in SCP

1. Investigator searches by the call type “Informant Line” within the specific time frame
2. Investigator retrieves results
3. Investigator can playback calls if authorized but CANNOT play back calls have been set up as Private
4. Investigator can ONLY see “unlisted” if the option was chosen during set up for the phone number
5. Station ID / Port Location is hidden if selected to be hidden during set up
6. The inmate ID or Pin is NOT shown on the CDR report
7. Investigator with CDR view access cannot view the set up in the Global List

Informant (offender) process
1. Inmate picks up the phone
2. Inmate enters language selection
3. Inmate enters either Speed Dial Code or Dialed Number as configured
   *system recognizes the call is to an “informant line” and does not ask for a PIN
4. Call goes out to the specified phone number
5. Live Investigator receives the call and is not required to accept the call or any admonishments, it simply connects
6. Informant is now connected with Investigator
Live Call Monitoring

The Securus Secure Call Platform (SCP) allows authorized users to live monitor calls in progress via any device connected to the Internet. The feature provides users selectable scanning of all live calls in progress, so the user does not have to scan phones that are not in use.

The feature’s integrated media player has a time shifting capability enabling the investigator to pause, rewind and replay even as recording continues. The investigator can replay any part of the conversation even after the call has ended.

SCP also allows authorized users to forward a call to an investigator and quickly identify calling patterns to the currently called number or phone in use.
Remote Call Forwarding Detection

Securus leads the industry in fraud detection and prevention and is pleased to offer real-time Remote Call Forwarding Detection (RCFD). Our RCFD solution can immediately terminate a call if it detects that a called party’s telephone number is call forwarded to another telephone number.

SCP can also allow the call to continue with one of the two following options if false disconnects are a concern:

- Announce to the inmate and called party that remote forwarded calls are not allowed, and mark the call in the call record
- Mark the call in the call record, without an announcement to the inmate and called party

The SCP user interface allows authorized users to create Call Detail Reports for those RCFD calls by selecting the “RCF” flag or using the specific termination code “Call Forwarding Detected,” as shown in the following graphic.
Covert Alert

The Secure Call Platform (SCP) includes the Covert Alert feature that will call an investigator on their cellular or another phone when a specific inmate places a call and offer them real-time monitoring of that call.

Configuring an Alert Notification

Covert Alert can bridge a call to an authorized remote number for dialed numbers, phones, or inmate PINs are under surveillance by investigators. The Covert Alert feature allows authorized personnel to monitor a call, from any location, while the call is in progress.

When a call is placed by an inmate, or to a phone number that has a Covert Alert trigger, it is automatically sent to the designated investigator phone number(s). A call can be sent to multiple numbers simultaneously allowing several investigators to listen to the call.
Covert Alert can send calls to any phone number within the facility or across the United States. Investigators can also monitor calls through on-site workstations using the S-Gate Live Monitor, or remote live call-forwarding feature. This allows facility investigators to monitor potential illicit activities regardless of the investigator’s location.

Covert Alert can send E-mails to the investigator(s) with information about a Covert Alert call including date, time, inmate PIN, originating telephone, and dialed number immediately after the called party accepts the call. The following figure provides a sample e-mail alert:

Alert Notification E-Mail

Investigators can also choose to receive a covert alert via text message. The text message includes the date, time, inmate PIN, originating telephone, dialed number, and an indication if the call has been recorded. The following figure provides a sample text message alert.

Additional Security Feature

For extra security, Coverts Alert can be configured to require a PIN to listen to the call. If activated, a customizable message will state, “This is a Covert Alert call from John Smith, an inmate at the DOC. To accept this Covert Alert call, please enter your investigator PIN now”:

“Barge In”

While on the covert alert call, the investigator can immediately terminate the call by pressing a predetermined code. Covert Alert can also be configured to allow investigators to enter a code and “Barge In” to the
call and speak to both the inmate and called party. This “Barge In” capability is available through both Covert Alert and on calls forwarded from SCP Live Monitor. When monitoring a conversation, the call can be forwarded to an investigator cell phone, office phone, or other designation, allowing them to barge into the conversation using the predetermined barge in code and acceptance digit.

**Covert Alert Call Detail Record Report**

The Covert Alert Call Detail Record Report allows authorized users to search for calls that triggered a Covert Alert. The report provides comprehensive detail regarding the call.

Covert Alert report results display critical information about each triggered alert such as who was alerted, what happened, call status, call start and end, duration, dialed number and more. By clicking the icon to the left of each record, users can display full call detail information for each call. SCP’s Covert Alert feature and reports have assisted in many criminal investigations throughout the country.
Crime Tip

The Securus Crime Tip feature is an inmate crime reporting tool that gives inmates an anonymous and secure way to provide crime tips to corrections officers. The Secure Calling Platform (SCP) system anonymously records all messages left on the Crime Tip Hotline, so inmates do not have to risk being identified as an informant.

Inmates can choose to report:

- Information about possible criminal activity, including narcotics
- A crime that has already taken place
- A threat to their safety
- Threats to the safety of others

While tips are anonymous as a default, informants may choose to leave their name.

The Securus Crime Tip feature includes:

- A pre-arranged telephone number (designated by the facility), provided to all inmates
- An option to listen to all or selected recorded messages
- An option to burn specific information onto CDs for use as evidence
- A way to generate reports of all recorded messages with the date and time of the message
- A way to leave an anonymous reply message to the inmate
Reverse Lookup

The Securus Secure Call Platform (SCP) reverse lookup feature identifies the billing name and address (BNA) of a dialed phone number captured in a call detail record. Users can easily point, click, and initiate a BNA search for the number in private and external data sources. This search process is unique in the industry, providing the most accurate BNA information possible.

When the search returns a positive match for a destination phone number, a pop-up box appears on the screen with phone number’s billing name, billing address, and the date the number was last verified. Unlike other similar tools in the industry today, the Securus fully-integrated reverse lookup feature is provided at no additional cost.

Reverse lookup allows users to access results from anywhere the number exists in SCP such as:

- Call detail reports
- Blocked number lists
- Global allowed lists
- Call frequency reports
Reverse Lookup and Personal Allowed Numbers (PAN)

If using PAN management, SCP allows authorized users to associate the BNA information to a phone number on the PAN list. This feature allows administrators and investigative staff to view BNA information without an additional search. The Securus reverse lookup feature offers a comprehensive ad hoc search tool giving an authorized user the ability to enter criteria ranging from first name, last name, address, city, state, and ZIP to obtain this information on demand.

Viewing BNA Information on an Online Map

Securus SCP integrates with Google Maps proving a quick and easy way see the physical location of the address associated with a telephone number. Highlighting any telephone number and clicking it renders a Google Map on the screen.
Mapping BNA Information

Users can activate GPS mapping functionality by combining the integrated BNA lookup feature with simple online mapping capabilities.

Point and click on a destination number to view the billing name and address for the number.
Scan Patrol

Authorized DOC personnel can use Scan Patrol to scan through live calls via the existing live monitoring function. Users can enter a specific amount of time the system will play each call before moving to the next active call, similar to the scan function on an automobile radio. The scanning begins from the first active call on the first active port and continues to the next active call, looping back to the first active call when reaching the end.

The following figure presents an example the SCP Scan Patrol page.
The Securus proprietary Location Based Services (LBS) product, the DOC can determine the true location of a cellular phone. LBS provides the following benefits to your facility:

- Provide the called party’s true location at the time of an inmate’s call via a link in the call detail record (CDR)
- Establishes a “Geo-Fence” perimeter around a location to notify investigators when an inmate calls a cell phone that is within the geo-fence
- Identifies the real-time location, on-demand, of a suspect’s cell phone (with appropriate warrant documentation)

Location Based Services
Securus’ Location Based Services provides correctional facilities, investigators, and law enforcement with the following benefits:

- Cell phone termination location at call acceptance and call end. **This means that LBS will tell you if inmates are calling someone right outside the prison walls.**
- Geo-fence perimeters or unlimited, custom boundaries that allow users to identify call termination locations within that fence
- Covert alerts that provide real-time notifications of call termination within a geo-fence
- CDR mapping of call terminations to wireless points
- Real-time location identification
Reports generated from the CDR contain an icon that identifies calls to a wireless number. LBS provides an additional link that maps the location of a wireless number when the inmate placed the call.

**Geo Fencing**

With geo-fencing, the DOC can set up a perimeter around the DOC facilities that identifies when an inmate calls a cell phone that is located within that perimeter at the time of the call. Geo-Fencing can generate a Covert Alert notification to investigators that allow them to act quickly on real-time information. This valuable capability helps protect your perimeter and is helpful in preventing escape attempts.

### Geo Fence Management

Covert Alert connects a call to an authorized remote number for dialed numbers, phones, inmates PIN, or geo-fence perimeters that are under surveillance. Authorized personnel can monitor a call from any designated location, while the call is in progress.

The investigator enters a telephone number (such as cellular, home, or office), which is where he or she wants the call sent to for live monitoring. When a call is placed by an inmate that meets the Covert Alert trigger criteria, it automatically routes to the pre-designated investigator phone number(s). A call can be sent to multiple numbers simultaneously allowing several investigators to listen into the call.
Real-time Location Services

Real-time cell phone location identifies the location of a suspect’s cell phone, in real-time, regardless of whether a call is in progress. This feature will aid investigators, with appropriate warrant documentation, in locating persons of interest faster and requiring fewer resources.

Location Based Services

LBS provides unmatched investigative value by showing you the geographic location where inmate phone calls are answered. Securus’ proprietary Location-Based Services delivers the following benefits:

• Increase the efficiency of your investigative staff
• Prevent and minimize contraband at your facilities
• Increase the safety and security of your community
Investigator Pro - Voice Biometrics

Securus has included new technologies that are not present in the inmate calling platform provided by the incumbent today. Our centralized, hosted investigative tools and analysis software will provide the Department investigators with a “roadmap” of suspected or suspicious inmate activity and will provide the Department the ability to easily access and share information.

Developed by JLG Technologies, now owned and operated by Securus Technologies Inc., Investigator Pro is a powerful evidence-gathering and investigative analysis tool that is proven and in use in facilities nationwide making corrections officers and communities safer every day. Investigator Pro is integrated with SCP and uses unprecedented state-of-the-art technology to “identify” the voices of all inmates speaking on telephone calls and exposes inmates who try to beat the system by hiding their identities using other inmate’s Personal Identification Numbers (PINs) to engage in criminal activity.

Securus Technologies announced the acquisition of JLG Technologies on June 11, 2014. JLG Technologies, LLC is the leading supplier of continuous voice biometric analysis and investigative tools to the corrections and law enforcement sectors. "We are very happy to be able to combine with JLG Technologies, LLC and their affiliates – Voice Analytics, LLC and JLG ICER Technologies, LLC," said Richard A. ("Rick") Smith, Chief Executive Officer of Securus Technologies, Inc. "They have the best continuous voice biometric technology in our industry – very sophisticated software that not only identifies unauthorized users on a particular call, but goes on to identify the user's identification." JLG Technologies, LLC currently has over 40 active patent applications at the U.S. Patent Office and expects the first of them to be issued within 12 months – so they have developed a valuable intellectual property portfolio."
Investigator Pro Continuous Voice Identification (CVI)

Investigator Pro’s advanced voice identification technology was originally developed for the U.S. Department of Defense. The Department of Defense was facing a huge challenge which was to find terrorist phone calls out of the millions of phone calls made every day to and from the United States. The U.S. DOD contracted with a major U.S. technical university with some of the best voice analysis engineers in the world to find a way to detect the phone calls. Over a 12 year period the engineers created a system to automatically monitor and analyze millions of daily phone calls and delivered a cutting-edge solution which today serves to help protect the U.S.

Investigator Pro analyzes inmate call voices immediately after the call has been completed. Alerts are instantly available to investigators in the real time status screen at the completion of each voice analysis. Every second of every call is analyzed. Investigator Pro does not use intermittent verification because this type of identification allows inmates to converse undetected by passing the telephone when the verification is prompted.

The Investigator Pro gleans a vast amount of data from the continuous biometric voice identification technology that can provide a wealth of high value intelligence information. The system is easy to use and all training is provided initially and throughout the term of the agreement to ensure your officers get the most value from the system.

As an additional benefit, Securus is the ONLY provider that can take that intelligence and import it into our industry leading THREADS investigative tool so that investigators have a full view of connections between conversations and inmate activities.

When used in unison with our other capabilities such as location based services and managed access services to control and monitor cellular telephone usage, customers are put in the best possible position to provide truly secure inmate communications.

CVI Actionable Intelligence

The Investigator Pro voice biometric identification system goes beyond continuous verification of one inmate’s voice. Investigator Pro continuously verifies the identity of all inmate voices that are speaking on a telephone call. Reporting of this fraudulent activity can easily be found with the QuickFind reporting tool. When accessing the QuickFind dashboard system, investigators will be presented with the “High Target Calls for Review” report showing the PIN that was used, the name or names of inmates whose voice print was identified during the call and name(s) of inmate that did not match the PIN being used.
The High Target Calls for Review report provides actionable intelligence by highlighting suspicious calls to make the most of an investigator’s time.

The system provides investigators with direct links to these recordings where inmates are attempting to hide their identity and provides the tools to review and annotate those conversations for further use in investigations.

Securus calls our service, Continuous Voice Identification (CVI) because we identify and report each inmate on the call and give you the names of the inmates. We do not just continually verify the inmate’s voice during the call. Most of our competitors can only continuously verify the voice of one inmate during the call and cannot report the identity of a second or third inmate that participated on the same telephone call.

The system’s easy-to-use dashboard automatically collects and analyzes a vast amount of information that would otherwise be labor-intensive to gather and interpret. This breakthrough technology changes the way evidence is gathered, shared, and used in the investigation and prosecution process. The Investigator Pro system provides the highest level of integrity, efficiency, and demonstrated effectiveness as an evidence case-management tool.

Anatomy of Investigator Pro™

Investigator Pro comes with an advanced Call Player, multiple reports, and even an interactive dashboard – all designed to provide investigators with the tools they need to exposes inmates who try to beat the system by hiding their identities to engage in criminal activity. The modules in Investigator Pro include:

- QuickFind™ – Puts critical information at your fingertips
- Voice Search™ – Find calls where inmate’s voice is found
- CallFinder™ – Filter calls based on dozens of criteria
- MyCallReview™ – Return to the calls important to you
- Suspicious CallFinder™ – Find all high-suspicion calls using analytics to make more of an investigators time
- NoteManager™ – View, filter, and create notes on calls
- ReportMaker™ – Run reports on various telephone system abuses
- Stats – View key messages and monitor analysis progress
As displayed in the screen print above, one of the most utilized modules of the CVI system is the CallPlayer Pro. This playback system gives you the power to play and annotate calls faster, with less duplication of effort by providing playback controls to split audio talk paths, speed up conversations or eliminate pauses. The system provides the following features:

- Ability to separate recorded voices and select only one voice to play back at a time
- Speed or slow a conversation or single voice within a recording
- User friendly playback module with intuitive buttons
- Saves time, allowing for more productive use of staff time, better distribution of staff resources, and cost savings
- Report feature allows for supervisory oversight, accountability, and assessment of your staff's investigative skills and activities

The use of the Call Player Pro can reduce a ten minute call, with all pauses removed and use of the other tuning adjustments, into a five minute call doubling the use of time spent on recordings.
Enrollment Process

The enrollment process is a vital part of securing a one time, high quality voiceprint from inmates. The two most important elements of any successful voice biometric identification system are excellent technology and supervised voice enrollment.

Securus will provide the fully-supervised enrollment of all Department inmates into the system. Supervised enrollment means that each and every inmate will be required to enroll their voice at an inmate telephone station under the supervision of one of our trained enrollers. The advantage of supervised enrollments is positive ID of each inmate to ensure complete credibility of the enrolled database. Unsupervised or poorly supervised enrollments can jeopardize the integrity of the voice biometric database. This enrollment can be achieved with minimal disruption and can be presented to the inmate as part of the overall new inmate telephone system introduction.

The process begins with extensive preparation by Securus and precedes the actual on-site enrollment by many days. Coordinated facility preparation is the key to success. Once at the facility, and immediately before the enrollment team enters a housing unit, our enrollment administrator will reconfigure that housing units phones from the normal call-out mode and place them into the enrollment mode via remote software. The enrollment team then enters a housing unit, announces instructions to the inmates, and begins the enrollment process. When all inmates have been enrolled, the administrator places the phones back into the normal calling mode. Priority should be given to intake facilities. As inmates are brought into the Department system, voice biometric enrollment should become part of the intake process. This will ensure that all inmates moving out of the intake/classification facility will already have voice print enrolled prior to entering newly assigned facility and will not require re enrollment. Securus will install dedicated enrollment phones at locations that best meet the needs of Department at the intake or other State facilities.

Securus is very experienced in voice biometric enrollments as we have enrolled over 250,000 inmates. A typical enrollment takes generally less than two minutes. Before the inmate is required to speak into the phone, the enroller checks the inmate’s ID tag against the facility’s inmate/housing unit location sheets.

The enrooler then enters the inmate’s PIN from the sheets into the phone keypad and instructs the inmate to say their name (as it appears on the sheets) and a short phrase, followed by a short paragraph of text. By doing this, the enrooler ensures that the inmate is who he says he is so that the voice signature is confirmed to be that of the inmate.

Our enroilers are experienced in assisting inmates through the process who cannot read and we will make accommodations in the enrollment process to support any individuals with special needs.
Investigator Pro ICER™ – (Inmate Inter-Communication Evaluation and Reporting)

After developing its Investigator Pro voice identification and crime investigation system now in place in 188 correctional facilities throughout the country, JLG Technologies, since acquired by Securus, furthered its research as a result of requests from corrections investigators to develop an automated way of identifying inmates who are illegally communicating with other inmates using the inmate telephone system. The end resulting solution was ICER our Inmate Inter-Communication Evaluation and Reporting system which uses our biometric systems to analyze and target calls which otherwise would likely never be found.

ICER enables detecting and reporting on inmate-to-inmate phone communications whether occurring within the Department’s own facilities state wide, or between inmates in the Department’s facilities and inmates in other participating jurisdictional locations or states nationwide.

The Threat

Inmates have been, and continue, to communicate with each other over the telephone systems that have been provided for their controlled contact with the outside world.

Until now, communication between inmates (each originating calls from inmate telephones) has essentially gone undetected because there was neither practical technology nor uniform networking capability to identify such communications. Following are highlights of the dangers caused by uncontrolled inmate to inmate communications:

- Through a variety of methods, inmates are circumventing the inmate telephone systems contracted by facilities to communicate with another inmate; whether the other inmate is in the same housing unit, a neighboring housing unit, in a different facility or in a different state. Inmates exploit conference bridges, services such as iPhones, Skype, Google Voice and other kinds of modern telecommunications technology. In addition, they rely on called parties to bridge the calls, place three-way calls, or even put two speaker-phones in proximity to one another, so that inmates can talk to other inmates.

- Until recently, inmate to inmate communication incidents were only found when accidentally located by correctional staff; however incidents are now known to occur with much wider frequency than previously known. ICER has already identified 1,000's
of these events for our partner facilities. Events that would have otherwise gone unnoticed.

- These uncontrolled inmate communications, often conducted by turning cell phones end to end to connect receiver with mouthpiece, have involved criminal activities including coordinating gang-related murders, drug trafficking and racketeering, as well as inmate disturbances at multiple correctional facilities around the country.

**Technology and Cooperation Provide Increased Safety**

Every day we learn from the news about instances of major crimes being solved because of the increasingly cooperative efforts of state and federal agencies that are now beginning to share case-critical data around the U.S. and the world. In the world of inmate phone calls, we are offering a new technology based on voice biometric analytics and a dedicated cooperative network provided through participating nation-wide correctional administrations. This combined effort will enable all participating corrections facilities and jails throughout the country to receive specific and detailed information on a call-by-call basis when their inmates are using their phone systems to talk to each other – whether the calls are connected between different inmate telephone systems, between pods in the same facility, or between inmates in facilities from Florida to Maine to California. The more agencies that take part in the ICER network and share ICER data, the more inmate to inmate communications events will get caught in the net and be reported.

- Until recently, inmate to inmate communication incidents were only found when accidentally located by correctional staff; however incidents are now known to occur with much wider frequency than previously known. ICER has already identified 1,000’s of these events for our partner facilities. Events that would have otherwise gone unnoticed.

- These uncontrolled inmate communications, often conducted by turning cell phones end to end to connect receiver with mouthpiece, have involved criminal activities including coordinating gang-related murders, drug trafficking and racketeering, as well as inmate disturbances at multiple correctional facilities around the country.
**How ICER Works**

ICER uses advanced voice analysis technology to generate a “call signature” — a representation of the call that does not involve any of the original audio — for each completed inmate telephone call. Call signatures are then automatically encrypted and transmitted to our central data center for analysis.

Because none of the original audio is used in a call signature, the ICER system is in full compliance with state laws regarding the transmission of call recordings.

Under normal operations, call signatures are created, transmitted, and received at the data center within seconds of each completed call. Upon arrival, the call signature is immediately analyzed and checked against other call signatures. If an inmate to inmate communication event is detected, it is logged in the ICER system database and investigators from the participating corrections administration are automatically alerted via email to log into the ICER system for the detailed report.

The ICER system doesn't require correctional facilities to transmit audio files and each agency is always in complete control of the level of sensitivity of any data transferred.
The ICER Event Report above is a sample of the reports that are received by Pennsylvania Department of Corrections (PA DOC) on a daily basis. This particular ICER Event Report shows that on May 24, 2015, two inmates from two different PA DOC facilities were found to be talking with each other around 8:00 pm EDT. The first inmate named Damion Floyd called telephone number 410-504-7254 and the second inmate, Natasha Miller called telephone number 724-471-6945 and was connected to Damion Floyd 180 seconds into her recorded session. The conversation between the two inmates lasted a total of 644 seconds. The ICER Event Report automatically generates actionable intelligence for PA DOC investigators on a daily basis. The PA DOC investigators value these leads and listen to each recorded call.

The ICER program is available to all Securus customers. If the Department decides to participate in the ICER program, The Department would receive the same daily ICER Event Reports.
If inmates from separate State run facilities (such as WA DOC and PA DOC inmates are communicating with each other), investigators at each State DOC would see inmate call data for their own facility (either on the right or left sides of the report). For privacy and security purposes, access to other agency information would require an automated request from the ICER portal to the participating agency, seeking permission to work with that agency to retrieve pertinent data about the second inmate. Where inmates are calling each other within their own facility, all data for both inmates will be displayed automatically.

ICER provides facilities with a detailed report of each detected inmate-to-inmate call event by means of a graphical user interface (GUI), so the facility can review the phone call involved in the inmate-to-inmate call event. ICER has been recently deployed in the Pennsylvania Department of Corrections with great success. We look forward to offering the same level of security to the Department’s facilities.

ICERTM – is a registered trademark of JLG Technologies, a fully owned subsidiary of Securus.

To offer further analysis of inmate calling and to augment the identified suspicious calls found with Investigator Pro, Securus has provided information on our THREADS analytics systems.
Securus THREADS

THREADS is a powerful, accurate, easy to use, investigative tool that will automatically analyze data such as inmate communication records, public phone records, and data from confiscated cell phones to automatically generate focused leads for investigators. Leads can include suspicious calling patterns, inner circles, communication events to numbers on a bounce list, associations between multiple inmates, correlations to called parties, and much more. Investigative staff can easily uncover patterns of fraternization between inmates and correctional officers, discover common contacts between inmates and called parties, and customize the information and reporting to exclude irrelevant data such as family or lawyers.

THREADS will detect criminal organizations being run from within jail, detect when multiple inmates are talking to one called party at the same time, find associations of multiple called parties based on who is calling them, and identify inmates who possibly have a contraband cell phone based on calling patterns.

All SCP calling data (such as call records, phone numbers, billing name and address) is automatically integrated into THREADS the moment THREADS is enabled for a facility. All other sources of data can be imported into THREADS and analyzed together in an investigation. For example, information from a confiscated cellular phone can be uploaded to THREADS, and analyzed with the corrections communication data to uncover potential criminal activity.
Access to more investigative data helps solve crimes and close cases. Securus THREADS is the most widely used investigative platform in the industry, with approximately 2,200 facilities installed, more than 1 million inmates served, and more than 1 million calls processed per day. With THREADS, investigators can share information with other law enforcement agencies (including other Departments, jurisdictions, and facilities) by granting secure access to your data. Likewise, other agencies can grant your investigators access to their data.

**Graphic Representation**

All information is presented graphically as well as in text.

*Interactive timeline charts and graphical analysis make it easy to reveal periods of high-intensity calling and other patterns.*

THREADS analyzes data and provides interactive visual tools to produce easy-to-understand reports, charts, interactive graphs, maps, and build evidence for use in a trial. Additionally, investigators can create customized alerts so they are notified when THREADS uncovers critical information.
Securus’ THREADS is a powerful investigative technology that no other provider can offer the corrections industry.
CorrectionsLink™

CorrectionsLink™ enables sharing of all inmate JMS, OMS, & ITS data across all CorrectionsLink county and state users. It allows investigators to obtain and confirm information about the offender that is entering their facility from all data entered in the current and previous JMS's in order to properly classify and house the offender.

State and Local Police Departments identify potential suspect lists based on information collected at crime scenes. District Attorneys, Prosecutors and Judges obtain information about an offender to support a successful indictment and adjudication process. Investigators (Corrections and Law Enforcement) utilize the CorrectionsLink™ as part of their investigations to look at patterns, known associates, and any additional information, especially as it relates to gang activity. Correctional Officers identify individuals visiting more than one offender in multiple facilities. Parole and Probation Agencies obtain additional information about their parolees.

CorrectionsLink was first installed in the Commonwealth of Massachusetts where it connects all 14 counties and the DOC. It helps the DOC's investigators and classification staff obtain information about an offender, regardless of the OMS / JMS in use at the counties and the DOC. This solution helps maintains the safety and security of officers and inmates.

CorrectionsLink™ supports the needs of the investigators and classification personnel at the connected counties by making the DOC's information available to them. In the Commonwealth, CorrectionsLink™ is used by over 200 agencies in addition to the DOC.

When deployed as a part of PublicSafetyLink™, the system includes visualizations such as trends, timelines, hotspots, etc., thereby combining vast amounts of information into actionable intelligence.

The following are the salient aspects of the CorrectionsLink™.

- CorrectionsLink™ performs a secure / federated search system of participating counties.
- The solution allows the counties and the DOC to maintain ownership of the data while making the information searchable.
- It enables the counties and the DOC access to share the following information:
  - Basic offender information: Charges, Alerts, Arrests, and Prior Incarcerations.
  - Scars, Marks, and Tattoos
  - Gang / Intelligence information
  - Visitor Information
  - Phone Data
• CorrectionsLink™ can also connect to other data sources such as state, local, and Criminal Justice systems data sources.
Guarded Exchange Call Monitoring, Reporting and Forensics

Our subsidiary, Guarded Exchange (GEX), understands the most important mission in the corrections industry is the safety and security of the institutions, the staff, the resident offenders, and the general public. GEX has developed the most comprehensive suite of investigative products and techniques capable of helping agencies predict and prevent illegal activity before it happens.

Founded in 2003, Guarded Exchange has developed over 70 proprietary software and hardware tools for the corrections industry. These products include iCons and an Investigations module with Actionable Intelligence Potential (AIP)™ predictive analysis. GEX software allows you to interface with information residing within your department’s database providing a comprehensive social link analysis.

Guarded Exchange has focused on investigative tools and strategies that aid correctional facility customers with gathering of intelligence, based on the interaction of the offenders with friends and associates. A key area of this intelligence-gathering is a technique known as behavioral analysis data mining. By the use of exclusive algorithms, Guarded Exchange searches for changes in patterns in offender behavior that may signal suspicious activity.

Working as a partner with Securus Technologies, Guarded Exchange has been monitoring inmate telephone calls for the Missouri Department of Corrections (MODOC) since November of 2011. During that time, we have developed over 6,000 separate cases of Actionable Intelligence for the Department and outside law enforcement organizations.

Securus will provide the GEX monitoring services and commit to active monitoring of at least 5% of all inmate telephone calls from within the DOC facilities. This service provides additional efficiency and productivity in discovering intelligence from the inmate telephone calls.

We accomplish this with over 70 proprietary technologies used to data mine through millions of phone calls, emails, financial transactions, and other information sources, to provide agencies with intelligence that counts. Because GEX is staffed by Licensed Private Investigators, agencies can rest assured that trained, professional personnel are the ones aiding in the investigations. While there are many investigative tools out there that point you in the direction of which offenders to investigate, Guarded Exchange’s technique is greatly enhanced by utilizing Live Analysts to monitor offender phone calls.
All actionable intelligence is formulated into reports and presented to investigators through daily interaction. These reports can be used to improve the efficiency and productivity of the investigative staff.

Guarded Exchange - Forensic Services

In addition to the monitoring services, Securus is proposing GEX forensic services. This service includes professional examination and data retrieval from contraband cell phones that have been gathered in the course of cell sweeps or investigations. These phones can provide invaluable intelligence that would otherwise be costly or onerous to obtain. The results and data extracted from these devices will be provided back to the Agency investigators within 24-72 hours.

Guarded Exchange currently employs Cellebrite UFED Touch certified users as well as a certified Digital Forensic Examiner and a licensed Private Investigator with over 4 years of experience in the field of data extraction, data analysis and cyber crime. With this unique resource and experience, GEX is able to extract data from the most difficult of devices. Often times, one tool is not enough and agencies should have a partner that knows the right tool to use at the right time. Guarded Exchange can also provide training and support for directly importing extracted data into THREADS (described above) or any other data analysis tools your agency may have available.
KIOSKS / TABLETS
OVERVIEW
About Securus Technologies

Securus has been in business for more than 29 years and is the largest inmate communications provider in the United States based on facilities served. We develop our own software, build our own systems, and maintain responsibility for the repair and maintenance of the equipment. Through our U.S.-based call center, Securus provides high quality, live customer service that reflects highly on our partner facilities and eliminates most calling community-driven complaints. Unlike our competitors in the industry, we use our own call center agents. We staff our state-of-the-art call center with more than 150 of our own trained and qualified customer service representatives.

Securus is a thought-leader in the evolution of technology for use in Corrections. We have designed, built, purchased or worked with the best technology solutions available with the purpose of providing our partners with a holistic solution to meet the ever-changing needs faced in Corrections every day. Securus has ensured that our platform has stayed future proof by regularly reinvesting in its enhancement. We invest more than $100 million annually to improve the capabilities of our platform to better support our customers. To ensure our partner agencies are never protecting their communities with obsolete systems, we have always upgraded them to our latest technology as it is released.

About JPay

JPay is a technology company located in south Florida with the single purpose of serving our nation’s federal, state, and county federal correction agencies. JPay has been providing technology solutions over the past 14 years, and is a subsidiary of Securus Technologies. JPay’s mission is to design easy and convenient ways to assist agencies in fulfilling their mission to rehabilitate offenders and reduce recidivism while keeping the facility and community safe. The JPay customer base includes corrections staff, offenders, and their family and friends.

Since its inception, JPay has been designing and developing cutting-edge solutions that facilities nationwide have implemented to achieve unmatched success. Products and services JPay has introduced to the corrections industry include electronic payments, release debit cards, email, video visitation, and handheld digital media tablets. JPay has statewide contracts in more than 30 prison systems. Specific to the expertise sought by this RFI, JPay has been developing digital media technology for almost eight years.
TECHNICAL SPECIFICATIONS OF THE TABLETS, NETWORK, SOFTWARE, AND SERVICES.

The JPay tablets features high quality construction with a shatter resistant, tamper-proof housing. They are built to stand up to the rigors of the inmate environment. This is evidenced by the 70,000+ tablets that we currently provide to agencies just like the DOC. The tablets are available in two sizes - the 4.3" JP5 mini and the 7" JP5S. The JP5 mini is available in two power options: alkaline batteries and a rechargeable, non-removable lithium power pack. The larger JP5S is rechargeable only. Each alkaline-powered tablet includes four new AA batteries at no additional charge. Rechargeable models include a clear battery charger at no additional charge. Accompanying the tablet is a clear 11-inch USB cable, clear plastic earbuds and a clear protective cover. The tablets have no camera or internet access capability.

Inmates can use their tablets to download and listen to music, download and draft email, listen to the radio, play games, read eBooks and more. Each device comes preloaded with the inmate’s name and ID. Main functions/features of the tablets include:

- **Education**
  Enroll and complete educational courses

- **Music**
  Search, preview and download songs and albums

- **Games**
  Download and play exciting, engaging games

- **eBooks**
  Search and download eBooks

- **Email**
  Read and compose email in privacy

- **Core Functions**
  Clock, Calendar, Calculator, FM Radio and PDF Viewer included in all tablets
Inmates can purchase a tablet directly from the kiosk in their housing unit. The cost is deducted from their trust account overnight. Within a week or two, the device arrives to the prison with the inmate's name and number already initialized. The inmate can connect it to the kiosk and begin downloading content right away.

JPay also provides each inmate 8GB of cloud storage at no cost, so they can choose which content they want on their device and which content they want to store in the cloud. Cloud storage holds an inmate's email, photos, VideoGrams, music, eBooks and education content. This feature also gives the inmates the ability to retrieve their digital content when they are released.

**Wireless Option**

The JP5 family of tablets also features the power of wireless technology. Instead of using a kiosk as a syncing point, the JP5 series can communicate with JPay servers through secure wireless access points. This effectively turns every tablet into a handheld kiosk that can send email, download media, order commissary, and send instant messages. The secure wireless capability can be completely disabled at the factory before delivery if the DOC prefers.

Wireless tablets also enable enhanced security. A constant connection to JPay's servers enables real-time monitoring of a device's status. For example, DOC staff can trace a device to the nearest access point to aid in locating. DOC staff can instantly lock and/or wipe devices remotely in the event of theft or other necessity. The operating system software is a highly modified version of the Android OS and has been revised at the kernel level to address the extreme security measures needed for operating in a corrections environment. The device drivers can only access JPay-validated access points, and cannot communicate with any other Wi-Fi networks or devices.
HARDWARE SPECIFICATIONS

The JPay tablet is proven in the corrections environment and is the widest deployed tablet solution available today. Hardware specifications include:

- 4mm clear impact-resistant polycarbonate shell with raised edges for impact absorption
- Capacitive multi-touch panel: 4.3” for JP5 mini, 7” for JP5S
- Screen resolution: 480x272 for JP5 mini, 1024x600 for JP5S
- High strength, impact-resistant security glass with integrated screen protector
- Quad core 1.5 Ghz processor
- 1 GB RAM
- 16 GB onboard storage
- Integrated RFID for device tracking
- Only runs approved applications (server-configured)
- Wi-Fi capable but requires JPay secure wireless access points installed in facility
  - Wireless function available at DOC request
  - Fraud lock and mortality timer
PHYSICAL SECURITY FEATURES, DIMENSIONS, BATTERY LIFE

Security Features:
- Each tablet is credentialed to the inmate who owns it and contains an embedded RFID chip that enables identification even if the device becomes corrupted.
- The inmate's ID number and name appear on the screen every time it is turned on, enabling staff to easily verify its owner.

Dimensions:
- JP5 Mini - 4.9" x 3.4" x .8"
- JP5S - 7.6" x 5" x .75"

Battery Life:
- JP5 Mini
  - Video (or any application where screen is constantly on): 10 hours
  - Music: 30 hours
- JP5S
  - Video (or any application where screen is constantly on): 7 hours
  - Music: 65 hours

OPERATING SYSTEM/SOFTWARE ENVIRONMENT

JPay tablets run a highly modified and secured version of the Android operating system. Our team of engineers has locked down the OS all the way to the kernel level, including the entire boot process. In addition, we have devoted significant time and effort in developing remote monitoring tools to track, support and update kiosks and tablets.

The inmate kiosk CPU runs a modified version of the Microsoft® Windows 7 operating system.

NETWORK REQUIREMENTS AND PROTOCOLS

JPay normally installs its own network, including establishing an ISP and running Ethernet cabling, conduit, and associated infrastructure. If the DOC provides network connectivity, all JPay would need is an available Ethernet connection and standard 110 VAC electrical power for each kiosk installed. Securus will install its proprietary design and network connectivity at no cost to the DOC.
USER INTERFACE

At the core of JPay's inmate services is the JPay inmate kiosk, which is the user interface for inmates to download music, draft and send email and eCards, attend video visitation sessions, log into their JPay account, and more. The JPay kiosk is the most time-tested, inmate-proof, multi-tasking kiosk to ever enter a prison space.

JPay designed each kiosk screen for ease of use and maximum accessibility. The screens and their flow are simple to understand and use, while the external and internal components are modular, allowing easy replacement. Kiosks are vandal-proof and are treated well because they provide a valuable service to the inmate population.
INTERFACE REQUIREMENTS FOR INMATE ACCOUNTING

JPay is the only vendor that can offer DOC a solution to process media transactions without burdening DOC staff members - the JPay Media Account.

*The JPay Media Account*

JPay can set up a virtual JPay Media Account for each inmate. Inmates (and family and friends, if the DOC desires) can fund the account, which inmates use to purchase tablets, music, accessories, eBooks and other digital content. The Media Account’s integration with the kiosk makes the buying process easy and fast. This of course, results in higher per prisoner media purchases and much higher overall adoption of the program.

JPay will interface with the DOC trust accounting system to receive inmate information. Each day, JPay will receive an inmate data file from the DOC via Secure File Transfer Protocol (SFTP) or via web services containing all relevant data for inmate identification such as the inmate’s name, ID number and housing location.

*Funding the Media Account*

Funds can be easily transferred from the inmate’s trust account to the JPay Media Account directly on the kiosk. This transaction can be set to process automatically or require the DOC approval for each order.
DATA SECURITY PROTOCOLS

JPay’s JP5 tablets use a highly secure version of the Android OS, complete with seven layers of software security that includes a secure boot loader, secure Linux kernel, mortality timer and a unique RFID. Hardware security features include a corrections-grade logic board and a highly secure USB port.

Each non-wireless tablet has a security timer that tracks the number of days since it was last connected to the kiosk. If the tablet is not connected to the kiosk within a specified number of days, it will lock and become unusable until it syncs with a kiosk again. Wireless tablets, since they do not need to be connected to a kiosk to download content and send/receive messages, can be set to lock if they are not detected by the Wi-Fi network for more than a specified number of days (default is usually 30). Along those same lines, wireless tablets can be instantly locked, unlocked, and located because of the wireless technology.

Kiosks are connected to JPay’s proprietary network; all JPay products allow only inmate communication with approved friends and family while prohibiting inmate to inmate communication, including connection to other tablets. In addition, in order for any content to be loaded to the tablet, it must be digitally “signed” by JPay, making illegal content a non-issue. Our network is hardened by a powerful firewall that allows access only to JPay’s servers.

We went in this direction with our devices as JPay realized quickly that the removable media model presents too many security concerns for prison and jail usage. Inmates can easily modify this type of tablet to accept non-approved removable media. Not only can nefarious content be found on the removable media, but communications can occur between inmates and contacts on the outside. Removable media is simply too dangerous. For this reason, JPay tablets do not have any removable media slots.
DATABASE ENVIRONMENT AND STORAGE

We install dedicated servers called Local Download Managers (LDMs) at each facility. The LDM’s sole function is to download digital content on demand from our Central Music Storage to the kiosks in each facility.

Inmates using our kiosks are never allowed access to our central music database. Instead, each kiosk must authorize and download all content from the LDM. Our in-house Network Operations Center (NOC) monitors each kiosk remotely and manages all aspects of its operation.

APPLICATION SECURITY AND AUDITING FEATURES

If anyone attempts to connect an unauthorized tablet to a kiosk, an error message displays and the tablet is fraud locked. For example, if an inmate logs into an inmate kiosk with his credentials but connects another inmate’s tablet to the kiosk, the kiosk will lock the tablet, rendering it useless. Any tablet not connected before its security timer expires will lock as well. This is customizable and can be turned on and off based on DOC preferences.

The kiosk’s sophisticated security management system lets JPay remotely monitor each unit and, if needed, update software or firmware and even reboot the kiosk. This type of access is unparalleled and requires a robust infrastructure to keep the system running without interruption. We recognize that the better the system works, the higher the adoption rate and inmate satisfaction.

In a wireless environment, the DOC would have extensive control and monitoring options via the secure online management portal called the Facility System. Staff will be able to lock a tablet on demand to prevent usage, as well as triangulate the location of a missing/stolen tablet to within a few feet. JPay tablets will arrive pre-configured for the assigned inmate; this configuration cannot be altered, so DOC staff will not need to change a tablet’s configuration. Staff can monitor a selected tablet’s real-time usage to prevent nefarious activity, even though unauthorized/noncompliant usage of JPay tablets is practically impossible.
EDUCATIONAL AND LEGAL RESEARCH

JPay has spent a considerable amount of time and resources in the development of its inmate educational programs and continues to introduce new content regularly. Its existing education platform, known as JPay's Lantern, leverages secure tablet-based content delivery to increase the availability, scale, and variety of existing educational programs. The open infrastructure platform is suited to building an education initiative from the ground up with courseware and educational partnerships. JPay's Lantern is a Canvas-based Learning Management System (LMS). Canvas is used by multiple education agencies and schools throughout the nation, and JPay has modified its website to produce a secure corrections-based LMS. The tool is proven and serves facilities nationwide today.

JPay currently partners with Ashland University in Ohio to offer college level courses designed by educational professionals from the corrections industry. The content is available for download to Ohio inmates' tablets once enrolled in a class. JPay's solution can support almost any content, including eBooks, study guides, college-level courses, and video coursework.

ACCESS TO COMMERCIALLY PREPARED INSTRUCTIONAL MATERIALS

The JPay tablet solution currently provides access to the following commercially-prepared instructional materials:

Khan Academy

Khan Academy is a not-for-profit organization that promotes learning through a wide variety of concise, easily understood “How to” videos. JPay offers the entire Khan Academy video catalog. Once a video is selected and downloaded, inmates can watch the videos on their tablet from their cell.

Khan Academy also offers a free GED prep course which is completely video-based, making it very easy to keep students engaged and focused.

Non-profit and Government Funded Courseware

Our platform also provides the best educational content from government organizations, non-profit groups and open educational resources. Offerings include numerous courses in Mathematics, Social Sciences, Natural Sciences, Humanities, as well as basic literacy.
**Custom Virginia DOC Content**

Securus and JPay will work with the DOC to assist in the development and addition of customized DOC content for our Tablet platform throughout the term of the agreement. Securus will regularly provide overviews of content added for other customers to allow the DOC to decide if the additional solutions are right for them.

**Law Library**

With regard to inmate access to legal information, our Securus SecureView tablet currently provides secure inmate access to a completely law library. The SecureView Law Library application allows inmates to educate themselves about their case, by finding state and federal cases, codes and litigations, jurisdiction specific codes, and more. This is one of the many features that will soon be integrated into the JPay tablet.

**Other Documents**

Our solution is expandable and has the capability to upload, store, and display authorized documents in PDF format. Document content is therefore unrestricted and could be used for facility handbooks, announcements, and other DOC publications. The DOC also has the ability to upload customize announcement for view by the inmates on the kiosk.

**ENTERTAINMENT (MUSIC, BOOKS, GAMES, VIDEOS)**

JPay tablets offer more entertainment content than any other tablet in the industry. We offer inmates the ability to download music, books, and games as well as the option to download and store approved photos.

**Core Functions**

Every JPay tablet comes standard with an extensive list of core applications, such as an alarm clock, calendar, FM radio, calculator, and a PDF file viewer.
Media Store

Inmates can use their JPay tablets to access the JPay Media Store to browse, purchase and download music, games and other digital content. Inmates simply sync their tablet with a kiosk to purchase and download their selections. Only DOC-approved content will be available in the media store.

Music

Inmates use the JPay inmate kiosk to preview, select, purchase, and download music. The music storefront not only shows the latest releases, top hits, and most popular albums, it also suggests other music a user may like, based on their previous downloads. From the kiosk or via the wireless network, an inmate can:
- Search by artist, album, and genre for over 11 million tracks
- Review descriptions of artists and albums
- Listen to a 30-second snippet of a song to make sure it is the desired version
- Browse the entire catalog in real time
- Download selected songs in as little as five seconds

Other key features of the Music application include:

Music Catalog Management

JPay's catalog of more than 11 million tracks is entirely free of explicit lyrics. This means that any music that has explicit lyrics will not be available to preview, browse, or purchase. The DOC can also restrict the catalog even further if desired. Using JPay's secure online management portal called the Facility System, DOC staff can locate a song on the catalog and delete it for any reason.

Mistaken Purchases Virtually Eliminated

Because our music platform lets inmates listen to music previews, view album art, and view album details, complaints related to mistaken purchases are minimized.

Purchasing Songs

Once an inmate is ready to purchase a song, they add it to their virtual shopping cart, agree to the transaction, and submit. The song will usually be available to download in the same kiosk session.
**Games**

JPay has recently released its latest application for tablets, a full-featured games store. The JPay Games Store is now available in eight state DOCs.

Other key features of the Game Store application include:

**Browsing the Game Catalog**

In addition to several basic free games that are pre-installed on each tablet (at DOC discretion), inmates can browse the JPay Games Store on their tablet for an ever-growing selection of educational and recreational premium game content, specifically geared toward the corrections environment. An inmate can read a description of each game before deciding whether or not to purchase.

**Purchasing and Downloading Games**

To purchase a game, the inmate clicks the "Buy Now" button to send the game to the virtual shopping cart for purchase. After the purchase is approved, the game will be available for download the next time the tablet syncs with the kiosk.

**eBooks**

The eBook Reader applications on the JPay tablet enables inmates to preview, buy and store thousands of books. Our eBook library includes more than 500,000 books from genres including classics, educational material, history and religious study. eBooks are available in several languages including Spanish, French, Russian, and German. Inmates search the catalog and select books to download to their device.

**Photo Viewer**

Included with every tablet is an application that lets inmates store and view photos they receive via the kiosk.

Friends and family can attach photos to their emails (as described below) and when an inmate syncs their tablet with the kiosk, they are able to store any photo attachments in their photo viewer to view later.
ELECTRONIC MAIL COMMUNICATIONS OPTIONS AVAILABLE TO INMATES

The JPay tablet offers a very comprehensive e-mail solution that embraces communications to decrease recidivism without sacrificing security. The solution, as further described below, allows the inmate to send and receive email from family and friends while permitting the DOC to implement security protocols to manage and control communications. Our base cost for e-mail communications has been provided within this RFI response.

Email

The JPay email application is not a standard SMTP-based system like Outlook or Gmail. It is a closed messaging system that keeps correspondence from ever leaving the JPay environment.

To use the application, a customer must access JPay.com or download our iPhone or Android mobile app. After creating an account, a customer can initiate an email conversation with an inmate.

Getting Started

Upon either visiting our website or installing our mobile app, a new customer starts by:

- **Searching for their inmate** - Searches are conducted using the inmate name or ID number
- **Creating a free account** – A verified email address and password are needed
- **Purchasing stamps** – Electronic stamps may be purchased in bundles to save money. Stamp cost is negotiated on a per-contract basis but is always less than the cost of an actual postage stamp.

Existing customers simply log into our website or mobile app to correspond with an inmate already linked to their account.

Sending Email

JPay’s email interface is clean and simple. Customers compose and send emails to a single or multiple approved inmates. A one-page email (about 5,000 characters) costs one stamp. Longer messages will be charged additional stamps and customers are asked to confirm the use of additional stamps prior to sending the email. Each added recipient adds one stamp to the cost.
**Photo Attachments**

Family and friends may send photo attachments with their email. Each photo attachment costs one additional stamp. Inmates view these attachments on the kiosk and can order printouts or simply download the files to the photo application on their tablets.

**The Inmate Experience**

When inmates receive email from friends or family members, they can use either the kiosk in their housing unit or their tablet to view and respond.

**VideoGrams**

VideoGrams are 30-second video clips shared between inmates and their friends and family. Similar to email, they are initiated by the customer and sent to the inmate via JPay's Android or iPhone mobile app. The inmate can view it on the kiosk and, in turn, respond with a 30-second video created at the kiosk.

Every VideoGram, both incoming and outgoing, routes through the Facility System, our secure online management portal. Depending on how the facility chooses to set up the VideoGram service, facilities can choose to have manual approval of each VideoGram coming in and going out, or have them delivered automatically (not screened by facility staff beforehand). All VideoGrams are still available for future viewing whether or not Auto Release is enabled. All released VideoGrams are displayed in the Facility System in the Mail tab (or "bucket", as it is known) under a section called "Released Video."
E-Cards

E-Cards enable customers and inmates to send each other expressions of love and caring in a new way. New E-Cards are constantly being added so that customers can send the right message at the right time of year or emotional expression.

We have found that providing E-Cards gives both customers and inmates a new way to communicate their feelings. In fact, when E-Cards first launched late last year, more than 30,000 were sent on the first day. Inmates can view E-Cards on the inmate kiosk or download them to their tablets.

LANGUAGE TRANSLATION

While the base function instructions of the JPay Tablet are only offered in English, inmates will have the ability to download any number of foreign language documents and music. Customized PDF documents can also be uploaded in any language.

ADAPTIVE FOR THE SENSORIAL DISABLED

JPay tablets have a built-in text-to-speech capability that transforms eBooks into audio books, which is ideal for inmates with literacy limitations. Several backlight colors are available, including black, which improves readability for vision-impaired users.

USER FEEDBACK PROCEDURES

Customers

In addition to the Help Desk options, user feedback options also include our Facebook page, our website blog and the JPay Family Forum.

These websites help customers with information about our company and how to resolve issues. It also provides avenues for input from other users who are in similar situations.

Hundreds of thousands of family members and friends have liked our Facebook page and post pictures and stories of their experiences daily, thereby providing mutual support and answering each other’s questions. Customers can also post any JPay-related question to our Facebook page and a JPay representative will contact them directly to resolve their issue.
**Inmates**

Inmates can provide feedback and get help through the built-in messaging system on the kiosk. They simply compose a message and it is routed to facility staff for approval and then to our Help Desk for resolution.

**DOC Staff**

The dedicated DOC account representative is always available via phone or email for DOC staff, regardless of the time of day or day of the week, to assist with any questions or issues that may arise. Securus will provide a dedicated full time staff member to support the tablet program and respond to inmate inquiries.

**CALLING RATES**

Under our Tablet solutions, the calling rates to use the tablet as a telephone are the same as the rates to use the traditional inmate telephones. We do not charge an increase in rate and would not increase the current rate used by the DOC as part of tablet/telephone solution. Additionally, all calling features, as well as security restrictions of the inmate telephone system, are passed through to the tablet such as required entry of a PIN and voice biometric identification continually throughout the call. Calls are recorded and tablet communications are available for live monitoring. Our existing tablet functionality is and will be specific to our SCP telephone system.
We have provided the following two references:

**Reference #1**

<table>
<thead>
<tr>
<th>Facility Name:</th>
<th>Ohio Department of Corrections and Rehabilitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address:</td>
<td>770 W Broad St, Columbus, OH 43222</td>
</tr>
<tr>
<td>Contact Name and Title:</td>
<td>Edwin Voorhies</td>
</tr>
<tr>
<td></td>
<td>Managing Director of Operations</td>
</tr>
<tr>
<td>Telephone Number:</td>
<td>614-752-1150</td>
</tr>
<tr>
<td>Email:</td>
<td><a href="mailto:voorhies@odrc.state.oh.us">voorhies@odrc.state.oh.us</a></td>
</tr>
</tbody>
</table>

**Reference #2**

<table>
<thead>
<tr>
<th>Facility Name:</th>
<th>New Jersey Department of Corrections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address:</td>
<td>1302 Stuyvesant Ave, Trenton, NJ 08618</td>
</tr>
<tr>
<td>Contact Name and Title:</td>
<td>Gary Alpert</td>
</tr>
<tr>
<td></td>
<td>Assistant Commissioner</td>
</tr>
<tr>
<td>Telephone Number:</td>
<td>609-826-5615</td>
</tr>
<tr>
<td>Email:</td>
<td><a href="mailto:Gary.Alpert@doc.nj.gov">Gary.Alpert@doc.nj.gov</a></td>
</tr>
</tbody>
</table>
GENERAL PRICING INFORMATION REGARDING THE TABLETS AND RELATED PRODUCTS, ALONG WITH THE VARIOUS DIFFERENT FUNDING MODELS OFFERED.

All JPay services would be provided at no cost to the DOC. Tablets vary in price depending on the model and optional features, from $49.99 to $69.99. Song, music compilations, and album downloads range from $1.29 to $19.99. eBooks range from 99 cents to $9.99, and games range from $1.99 to $9.99.

ONSITE AND OFFSITE TRAINING

Implementation Training

For initial training, JPay provides instructor-led classroom training for large or small groups of DOC employees. This can be performed at a central location or on a facility-by-facility basis. Our goal is to ensure attendees have an opportunity to ask questions and become familiar with all aspects of the hardware, infrastructure, and management tools. JPay generally gives an in-depth overview and then analyzes real world examples, showing how various elements come together to create solutions to existing problems.

Ongoing Training

Refresher training is provided in person or through web-based programs, depending on DOC preference. We use these remote tools to assist staff with computer-based training and remote guidance. This training is also used if additional services are implemented. Securus will provide training at any time upon request of the DOC.

Training Materials

Training manuals and tutorials will be provided to each facility and are also available on the Facility System or can be distributed via email. The materials are distributed during and after training sessions, before software releases and during campaigns to promote learning and adoption of features. These materials are always updated to reflect any software or feature updates.

Manuals

A user manual comes preloaded onto each tablet in both English and Spanish that explains how to use all of the features and apps. JPay has also developed written and video training instructions for inmates on how to use all of the JPay-provided services, including the inmate kiosk. Kiosk tutorials are available in the Help section where appropriate.
HELPDESK OPERATIONS

JPay operates a 150-person call center 24 hours a day, 7 days a week, every day of the year that provides customer support for all inmate family members and friends. For DOC support, we will designate an account representative and a help desk analyst, both of who will be available full-time to address any questions. In addition, our help desk support team can assist with ad hoc inquiries, reports or questions.

24/7 AND 365 SUPPORT PROCEDURES

JPay’s call center is operational 24 hours a day, 7 days a week, every day of the year to provide customer support for all inmate family and friends. JPay will assign a dedicated account representative and help desk analyst, both of who will be available to the DOC staff 24/7 to address any questions.

FREQUENCY AND ACQUISITION OF UPGRADES

You cannot solve tomorrow’s problems with yesterday’s technology. Securus invests heavily in our technology. We have implemented an average of 50 upgrades per year to our Secure Communications Platform and are as focused on our Tablet programs. We are continually expanding applications that can be uploaded to existing equipment.

JPay’s development team uses Agile-based scrum development, which means we work in short sprints to build software components. With software releases every few weeks, we can stay flexible and adapt to customer needs as they evolve. If an upgrade involves tablet-based software, the upgrade will install automatically when an inmate connects a tablet to the kiosk.

Since 2011, we have made significant investments in acquiring and developing technologies to broaden our product offerings to include solutions for the entire civil and criminal justice industries.
MANAGED ACCESS SYSTEMS (MAS) OVERVIEW
Securus Managed Access Solutions (MAS)

Why Securus?

Through the extensive staff experience, the procurement of technology leading companies and strategic technology partnerships, Securus Managed Access Solutions (MAS) experience is visible in a significant number of the currently deployed MAS solutions within the USA today.

The Securus team of subject matter experts understands the challenges of the Radio Frequency (RF) environment that a prison environment presents. Securus understands the challenges because our team members have worked in this environment and gained the expertise required to accomplish a successful implementation of a Managed Access Solution in a secure facility.

Nothing beats real-world experience and Securus’ team has been involved in many deployed MAS solutions within the US correctional market, including one of the largest deployments in the nation for GA DOC. While some providers can speak to hypothetical deployment scenarios, Securus can demonstrate active competence in MAS technology, implementation, and deployments.

Most significantly our approach includes:

- Define Project Success - Goals & Objectives Up Front with Corrections
- Approach with perspective - Each Facility is Unique
- Determine Target MAS Coverage Areas
- Perform initial Site Survey
- Provide a Scope of Work (SOW)/Project Implementation Plan
- Receive Final Review and Sign Off by Corrections
- Receive letter from Corrections to commercial mobile carriers
- Commission a Joint Implementation Team
- Project Management
- Milestone Steps and Progress Completion
- System Commissioning
- Test and Turn-Up
- Operational Readiness
- On-going Maintenance and Support
How it Works

The Securus MAS initially captures all phones in the restricted areas by transmitting cellular signals that appear to be the commercial carrier network(s). In order to provide service for facility-approved phones in restricted areas, phones are divided into two categories: authorized and unauthorized.

Authorized phones are maintained in a secure “watch list” database that is created by the facility and managed by Securus. All other phones are unauthorized. The watch list database is checked as each phone registers on the Prison MAS network. If a phone is authorized, it is rejected and not allowed to be held on the Prison MAS, which allows the handset to re-connect to the phone’s commercial provider service as it would normally connect.

Unauthorized phones are permanently held on the MAS network and are unable to get cellular voice, short message service (SMS/text) or data services.

In addition, all unauthorized voice calls or SMS attempts receive a customizable recorded voice or SMS response, respectively, indicating the user is in violation of facility communications policies or laws.

The only calls that the Securus MAS system completes are E911 calls. 911 service is provided for all captured phones. 911 calls from unauthorized phones will be routed to the facility’s master control station, while 911 calls from Authorized phones, which communicate via their carrier network, will be routed to the local public safety answering point (PSAP).

System Architecture

The Securus MAS solution detects, identifies, and manages cellular communications, providing detection and management of any mobile cellular handset communications from all major carriers and all mobile handsets using any commercial cellular frequencies/bands and protocols available today in the USA.
The figure below shows the overall system architecture for the proposed Securus MAS.

MAS System Architecture

The Scanner/controller decodes the protocol on 2G, 3G, and 4G (LTE) frequency bands to enable the controller to set parameters to a series of remotely configurable radios. The decoded protocol parameters from the commercial base stations control channels are analyzed and the appropriate configurations are determined to enable the system software to provide cloned base stations which both attract contraband mobile phones to the prison network and appear to the contraband mobile phones as its normal commercial carrier.

The base stations are configured via the system software on the workstation and provide the ability to interact with cell phone handsets, as well as provides the policy engine to set policies on how and what to do with the mobile handsets once they are captured onto the Securus Managed Access System.

In order to provide adequate and focused coverage, as well as remain compliant with the FCC and carrier requirements of coverage areas and signal levels, the base stations are integrated with a Distributed Antenna System (DAS). Each DAS is custom designed for each installation and facility. The DAS distributes the selected commercial carrier cloned base station signals, throughout the designated areas within each facility, and provides a private cellular telephone network within the prison or jail. The Securus MAS cell phone network is separate from the commercial cell phone network, but similar in form, function and design. At no time does the system affect the RF or cellular environment outside the facility.
Remote Access System (RAS)

The Securus MAS system is remotely controlled via a Remote Access System (RAS). This design implements the most secure virtual private networking processes through dedicated IP access equipment. The system provides for the majority of all operational and maintenance tasks to be handled remotely, thus significantly reducing technician visits to the facilities and the resources to support the visit by the DOC. This design also allows technicians to remotely monitor each system 24/7/365 from one of Securus’ Network Operations Centers (NOC) and support and service the VA DOC every hour and every day of the year.

Second-to-None Support

Managed Access Solutions requires continued and consistent care and feeding to ensure your jail experiences the full benefits of the solution. That’s why we continuously evaluate the performance of our MAS deployments including:

- Infrastructure Review/Site Survey
- Radio Frequency (RF) and Distributed Antenna system (DAS) Design Plan
- System Test and Commissioning
- Operational Status and Life-Cycle Support
- Remote Management
- Technical Support included
- site visits planned/scheduled
- Securus monitors the MAS system 24/7/365 (Dallas– Network Operations Center)

Benefits

- Securus Managed Access supports 2G, 3G, and 4G (LTE) technologies and protocols used by US Wireless Cell Phone Carriers to ensure maximum coverage.
- Automatically detects the commercial carriers and technologies being used at a particular facility location
- Capable of decoding messages to and from mobile phones to register them on the prisons private network or MAS
- Actively identifies and manages all mobile devices 24/7/365 days a year.
- Prevents unauthorized devices from obtaining commercial mobile carrier network access
- Logs all mobile phone operations for future investigative actionable intelligence
- Provides Audit Trail for security purposes and reporting
NOC Live Monitoring

All of Securus MAS operations are supported by a 24x7 network operations center, to include:

- continuous system monitoring and problem resolution
- 24/7/365 NOC with Two facilities being monitored
- help desk and trouble reporting
- authorizing approved devices
- assistance in report generation / intelligence gathering

NOC Live Monitoring of MAS Installations
Combining Technology, Reliability, Service and PEOPLE to meet the needs of Cell Phone Managed Access Services in the Virginia DOC

Securus has created a comprehensive Managed Access Solution (MAS) to meet and exceed the needs of the VA DOC and provides innovative approaches to resolving challenges faced by the DOC. The following information details a cell phone managed access solution to effectively eliminate contraband cell phone communications use within the Virginia DOC facilities. The challenge for the DOC is to select the Cell Phone Managed Access system that offers the most comprehensive package of technology, service, support, and experience.

Proven Capabilities of the Proposed Solution

Securus’ Managed Access Solutions (MAS) is designed to prevent/block and manage illicit cell phone use in correctional facilities, and secure government compounds.

Securus may be a new name in the Managed Access marketplace, but the components that make up our MAS team certainly are not. Securus, thru acquisitions and acquiring experts in the necessary disciplines, has assembled a unique TEAM and technology offering with the most experienced staff in the industry.

The foundation of our MAS division is the acquisition of Cellblox which had been in the MAS development phase for over five (5) years and has systems deployed and operating in Georgia. Add to that the exclusive rights to the technologies and expertise of VANU Tactical, with more than five (5) years hands-on MAS experience in California, Mississippi and Texas and you have an unmatched level of knowledge regarding cellular and radio frequency management in correctional facilities. Additionally, Vanu is an actual commercial carrier with systems deployed to enhance the back roads of the USA and other international areas as a commercial carrier. Securus is committed to developing new technologies and creating more cost-effective Corrections-specific MAS systems to promote contraband cell phone solutions in the marketplace.

Securus is interested in a long term partnership with the DOC to combat the Cellphone problems in all areas and all facilities, Securus is deploying several MAS systems currently and where appropriate, Securus is also offering services for Cellular phone forensics and investigative services to support the DOC. We recognize there is more to contraband cellphone investigations than simply managing the transmissions and we are focused on supporting the DOC in all aspects of this problem.

Securus will work with the DOC, as a partner, to identify contraband cellphone issues specific to DOC and engage our team of subject matter experts, both inside and outside of
the company. Our knowledgeable team will be available to assist the DOC in any and all aspects of Cell phone issues that are current today or that we discover in the future. Securus strives to be the very best partner in the fight against contraband cellular telephone issues.

Securus is currently providing MAS service within the Georgia Department of Corrections (GDC) at three of the GDC prisons (Macon, Smith and Telfair). Most recently the Smith State Prison was upgraded with the latest software resulting in attaining the stated goal of Georgia Department of Corrections – “make the contraband cell phones useless to the inmates.” In addition to simply managing the cell signals from within the facilities, there is valuable intelligence information being gained by the GDC from the reporting features of our system.

Deployments at all three sites in Georgia include the capability to manage all cell phones, including 4G LTE smart phones; an industry first in a State DOC setting. GDC has fully accepted all three sites as operational and Securus has provided supporting information to prove reduction in the proliferation of illicit cell phone events along with a correlating increase in the call traffic using the installed Inmate Telephone System.

Securus MAS is a combination of a uniquely managed cellular telephone system network and a tightly controlled Distributed Antenna System (DAS). Securus MAS is capable of 2G, 3G, and 4G (LTE) technologies and protocols used by all U.S. Wireless cell phone carriers. The system is also fully compliant with all Federal, State and Local laws and regulations. Securus MAS allows corrections facility representatives to effectively manage contraband cell phones without impacting legitimate wireless communications within the designated areas of the prison.
The Securus Managed Access Solution offers:

- The installation of a combination of a specially managed cellular telephone system network and a tightly controlled Distributed Antenna System (DAS).
- A MAS solution capable of detecting 2G, 3G, and 4G (LTE) technologies and protocols used by any and all Wireless cellphone carriers within the USA.
- The ability to manage mobile devices and applies policy rules as determined by the DOC administrators to either allow or disallow cellular communication
- The ability to respond to changes in technology and adapt to those changes without additional cost to the DOC.
- A fully automated solution which manages all cellular telephone access 24/7/365 days a year
- Complete administrative control capabilities both locally and remotely.
- 24/7/365 active monitoring, support and service through the Securus Network Operations Center.
- Total Securus-managed solution requiring little or no special training, additional staff or significant commitment of time by DOC personnel...TRANSLATION: Easy to use and understand!
- Saves considerable amount of resources (direct cost savings) for handling Contraband cell phone issues within the facility as the MAS manages communications automatically 24/7/365 and blocks voice, text, and data that were possibly creating many other issues.

The Securus MAS provides multiple benefits to correctional facilities, including:

- Improved safety by limiting illegal inmate communications
- Lower costs by reducing the time and money required to detect and deal with issues involving contraband cell phones.
RECOMMENDATIONS
Recommendations Regarding Implementing Inmate Telephone and Investigative Systems.

A successful Inmate Telephone System (ITS) should be centralized in nature to ensure data integrity and promote disaster recovery success.

A successful ITS should be web-based and able to be connected-to from any internet enabled PC or device without the need for additional VPN or other separate (third-party) connections or hardware.

A successful ITS should offer the native ability to identify the location of cell phones that have received a call from the inmate telephone system. This information should be presented in map form to allow staff and investigators easy access to usable information.

A successful ITS should offer a voice biometric that not only identifies inmate voices at the beginning of calls, but also identifies all inmate voices throughout inmate telephone calls.

A successful ITS should provide the ability to search inmate calls based on inmate name and inmate PIN as well as by inmate voice print. This expands the investigative capabilities of the system and provides DOC the ability to identify ALL calls from a particular inmate, even if they are not using their assigned PIN.

A successful ITS should be supported by a US-based customer call center and 24x7x365 technical support in order to reduce or eliminate the need for DOC staff to accept or respond to constituent complaints.

A successful ITS should be combined with a data analytics package that has been designed specifically for law enforcement and corrections and works proactively, rather than reactively, to identify patterns and linkages between inmate calls (and any other relevant data types) in order to create efficiency and actionable intelligence for investigators.

A successful ITS should provide the ability to initiate automated alerts when a specific inmate PIN is used or a specific telephone number is called. These alerts should be available in the form of a call to a separate staff phone or cell phone as well as an email with details pertaining to the alerted call.

A successful ITS should identify any calls that indicate inmate-to-inmate communication, regardless of whether or not the inmates dialed the same telephone number AND whether or not both inmates are housed within the same facility.

A successful ITS should interface with the Offender Management System to automate the creation and management of inmate PINs to include inmate name, PIN, housing location and other similar demographic information.

A successful ITS provide authorized users with the ability to extend the storage duration for recorded inmate calls in order to assist with longer term investigations.
A successful ITS should provide users with the ability to create virtual folders when “downloading” recorded calls with the enhanced capability to email a link to the virtual folder, providing expedited access to recordings for outside agencies without sacrificing the security of the DOC’s data.

A successful ITS should provide the ability to display the available billing name and address for the telephone numbers called from the inmate telephones.

A successful ITS should provide an enhanced call player which offers authorized users time saving techniques when playing back inmate call recordings. These techniques should include: speed up or slow down the call recordings without distortion or pitch shift, split the call to listen to only the inmate or called party side of the recording, skip the pauses and display the amount of time saved when any of these features are activated.

A successful ITS should offer an enhanced call player that provides a visual indicator of the location of three-way call events within the inmate call.

A successful ITS should provide users with the ability to create custom Security Threat Groups, associate specific inmate PINs to a particular STG and search for calls by STG rather than individual inmate PIN.

A successful ITS should allow users to monitor all inmate calls in real time with investigative features such as quick find for the last ten calls to a monitored number or the ability to forward a monitored call to an outside telephone number.

We recommend that prior to any implementation of systems that the DOC work with Securus’ Project Methodology team and discuss or complete the six key phases that are essential to any successful system design. The six phases include:

1. **Targets:** This phase assesses the need for change, determines readiness of the organization and defines the scope of targeted changes to support the organization’s growth strategy. The goals and strategic project objectives are identified, clarifying expected outcomes, which are qualified by key stakeholders.

2. **Planning:** This phase is very important as it aligns the project approach with the organization’s strategy (targeted changes). *Time spent on planning saves hours* in the project and insures the strategic targets and objectives are met.

   The project Kick-Off meeting occurs during this phase. The initial meeting with all project team members and key stakeholders is held. Roles, responsibilities, policies and procedures are reviewed to insure DOC guidelines are followed throughout the project. **Communication** protocols and escalation procedures for issue resolution are established.
The project plan targeted objectives, milestones and resource allocations are defined/revised to insure all activities are identified to achieve project success.

3. **Knowledge Transfer:** This phase is at the heart of incorporating new software into the organization. During the Knowledge Transfer phase of the project plan, classroom training of SCP's capabilities occurs. Discussions are encouraged to define known constraints or gaps. During this phase, the ‘how’ is developed for each requirement, documented and embraced.

4. **Implementation:** An iterative process, implementation overlaps with Planning, Knowledge Transfer and Transition. The project plan is executed with identified resources, maintaining the project schedule, managing project scope changes, and project issues. DOC stakeholders actively participate in decisions that impact the culture and expected outcomes. This phase is focused on delivering project objectives, products, services and results expected by the DOC.

5. **Transition:** Transition is an activity-rich phase where project tasks are completed to meet the objectives of each functional area. Communication and ownership are key to completing this phase with confidence. At this point, final testing for data conversions, load testing, interface testing and unit testing occurs. Production environment is readied. Cutover activities planned weeks in advance are activated. The SCP is live and the implementation is complete.

6. **Continuous Improvement:** The final phase of Continuous Improvement is ongoing. A partnership between the DOC and Securus has been developed and is continual. As Securus develops new enhancements, incorporates new technologies and creates new products, the DOC will benefit. Continuous Improvement is not just a phase; it’s a way of life.

We recommend that all new systems be built and installed in parallel operation with the current systems to ensure proper functionality prior to transition.

We recommend that Securus technicians migrate technology after hours when inmates are in lock down, thereby minimizing revenue loss and facility impact.

We recommend that all system integrations be discussed with Securus technicians prior to system installation. Securus technicians have extensive experience integrating our products with other, commonly-used facility technologies, including commissaries, trust accounts, and jail management systems.
Recommendations Regarding Implementing Kiosks And/Or Tablets.

We recommend using a model in which the tablets are shipped to the facility "blank" and are credentialed to the inmate when first synced with a kiosk. This approach increases security while enabling easy distribution. If wireless is not implemented, we recommend a model in which content is delivered through the kiosk when the inmates sync their tablets, since this method minimizes staff involvement.

JPay recommends a model in which the music catalog is accessible via the kiosk as well as the tablet. The kiosk-based catalog is larger and updated much more frequently and enables song previews before the user makes a purchase decision, therefore reducing mistaken purchases. When an inmate cannot access the kiosk, they can still browse their tablet-based catalog to select potential songs for subsequent purchase and download.

The music catalog should offer inmates multiple ways to search for music, such as by song name, album name, artist, and even music genre. Also useful is being able to see the current top-selling albums and songs.

Cloud storage is also an advantage, since it lets inmates transfer music between their tablet and their allotted amount of cloud storage. This prevents tablets from reaching their storage limits, which would curb future purchases.

We recommend the use of a "wish list" for saving songs for future purchase, since an inmate may not always have sufficient funds in their account to be able to purchase all desired content.

Tablets should include security features such as requiring the user to enter their PIN before use and having the tablet lock if the user attempts to connect it to an unauthorized device, such as another tablet or a computer.

Inmate kiosks should employ a physical keyboard, not just a touch screen. Many inmates do not own tablets and compose emails directly on the kiosk, and a physical keyboard greatly simplifies and speeds up data input.
Recommendations Regarding Implementing Managed Access Services (MAS).

A successful MAS should utilize a distributed antenna system, rather than a single antenna system. This provides for a more controlled management of the cellular signals, without interfering with signals in public areas.

A successful MAS should detect and manage 2G, 3G and 4G (LTE) spectrums, at minimum. Without proper management of LTE signaling, there is opportunity for devices to circumvent the MAS system and undermine the control of the wireless signals.

A successful MAS should be monitored 24x7x365 from a centralized Network Operations Center. Without proactive monitoring of all aspects of the system, including each individual node on the distributed antenna system, facilities leave themselves vulnerable to cellular signals escaping due to a single faulty device, possibly without any notice or visibility that a device has failed.

A successful MAS should be scalable and expandable to accommodate for changes in technology and spectrums. Without future scalability, a MAS system is likely to become stagnant within just a few years, making it a bad investment.
Your Single, Trusted Source for Integrated Solutions

VIRGINA DEPARTMENT OF CORRECTIONS
RFI No. DOC-16-079
Inmate Electronic Communication Systems

Presented to:
Virginia Department of Corrections
Attention Peter Bratley, Procurement Manager

Presented by:
Thomas J. Gibney
Account Executive
Telephone: 814-330-3830
Email: tom.gibney@gtl.net
Alternate Email: RFP@gtl.net

The Corrections Innovation Leader
April 1, 2016

Mr. Peter Batley, VCO, CPPB  
Commonwealth of Virginia  
Department of Corrections  
Procurement and Risk Management, Room 2150  
6900 Atmore Drive  
Richmond, VA 23225

RE: RFI No. DOC-16-079 for Inmate Electronic Communication Systems

Dear Mr. Batley,

Enclosed with this letter is Global Tel*Link’s (GTL’s) response to your issued RFI No. DOC-16-079 for Inmate Electronic Communication System for the Virginia Department of Corrections (VADOC.) We appreciate the opportunity to present the DOC with information on our industry-leading Inmate Electronic Communication Systems via our enclosed RFI submittal.

The decision to select a partner requires careful consideration regarding who offers the best combination of experience, technology solutions, training and support. GTL has been that partner working closely with the Virginia Department of Corrections for over 24 years now. We commend the VADOC in doing its diligence in gathering information and specifications for an inmate electronic communication system that properly aligns with the overall vision for the future of the Department.

Should you have any questions concerning our response or need additional clarification, please feel free to contact me directly at (814) 330-3830 or via email at tgbney@gtl.net. As an alternative, Anthony Pellegrino, Vice-President of Mid Atlantic Sales can be reached at (814)-515-1760 or via email at apellegrino@gtl.net.

In closing, I want to thank you, the Commonwealth of Virginia and the VADOC for the opportunity to provide our response to the issued RFI for Inmate Electronic Communication System.

We have enjoyed a long successful partnership with the VADOC and look forward to expanding upon that for years to come.

Sincerely,

Thomas J. Gibney  
GTL Account Executive
| Table of Contents |

A. | Technical Specifications and Features  
B. | Security Features  
C. | Hardware and Software Updates  
D. | Commissary Ordering  
E. | Kiosk to OMS Integration  
F. | Kiosk and Tablet Applications  
G. | Financial Models  
H. | Implementation Recommendations  
I. | Company Information  

© 2016 Global Tel*Link Corporation  
Virginia DOC RFI #DOC-16-079 | Table of Contents | 1 of 1
A. | Technical Specifications and Features

Virginia Department of Corrections
TOPIC: Technical specifications and features of the inmate phone system, kiosks, IT network and related services, along with technical specifications of the managed access system.

Tablets

Inmate handheld tablets have been gaining acceptance and penetration in the industry for the past year. This cutting-edge technology has also been met with great scrutiny and skepticism within the correctional industry at the same time. GTL has found that a successful tablet program can only be delivered when the solution is properly aligned with the goals and objectives of the Agency while simultaneously addressing security as a key consideration.

GTL’s tablet program is definitely aligned with the security concerns and objectives of DOCs. This is well proven and documented—as GTL has never lost a successfully installed tablet program or had a client cancel. Determining a vendor’s lost / cancelled accounts is an important part of any tablet program evaluation; to avoid making the same deployment mistakes that others have made.

Inspire™ Wireless Inmate Tablet

GTL is pleased to provide the VADOC with information about our Enhanced services solution featuring our Inspire™ wireless inmate tablet and multiple applications that provide:

- Communications for Inmates – phone, email, and in the near future: instant messaging.
- Inmate educational and information services.
- Facility Services including the distribution of facility information; commissary ordering, handling inmate requests and grievances. GTL is the ONLY vendor that can provide these services while directly integrating to the new GTL Offender Management System currently being implemented.
- Inmate entertainment – music, games, books, etc.

As part of our Enhanced Services solution, GTL’s created the Inspire wireless tablet exclusively for corrections. This integrated product offering uses cutting-edge technology to allow VADOC inmates the safe usage of corrections-grade handheld tablets through our secure Wi-Fi network as a multimedia communications device, which includes making telephone calls directly from their housing units/cells. GTL’s solution allows mobile communication and features while still providing the safety and security protocols that VADOC requires.

GTL was the first to put a tablet with calling capabilities in an inmate’s hand. We have the most experience in deploying secure inmate tablet systems.
The Inspire Wireless Tablet – Future of Inmate Communications

The Inspire wireless tablet provides phone calls, email and future features such as instant messaging. Society is changing the way in terms of how we communicate. If inmates can only make phone calls in a society that shuns phone calls in favor of email, recidivism could rise due to limited opportunities of interaction with their loved ones.

Technology is changing the way society communicates.

Inspire Wireless Tablet Specifications

- Screen: Capacitive multi-touch screen
- Communications: Wireless 802.11 b/g/n
- Memory: 512Mb w/ 8Gb flash
- Power: Li-Polymer battery pack
- Ports: (1) 3.5mm RCA Jack Audio In/Out
  (1) Micro USB 2.0 port
- Charging: (1) AC 5V 1.5A power port
- Functions: On/Off button; Volume +/ - button
- Security Features: Secure OS, secure case
- Accessories: The tablet comes w/ a clear power adapter and headphones.

Dimensions: 7 ¾” height; 4 7/8” wide; and ¾” thick.

Our tablets are custom built by GTL with a secure operating system, offering vastly superior security over product offerings based on stock “off-the-shelf” tablets. GTL built the enhanced services tablets from the ground up blending our custom-built OS with secure, durable hardware ensuring only GTL software can function on the hardware and vice versa. GTL’s unique operating system supports multiple audio formats including MP3, WMA and WAV and video formats including MPEG2/3/4, H.263/H.264 with resolution up to 1080p 60fps.

Built for Corrections

Inspire tablets have a durable, clear, corrections grade body to prevent contraband from being hidden inside the case. Our tablets are custom built by GTL with a secure operating system, offering vastly superior security over product offerings based on stock “off-the-shelf” tablets. GTL built Inspire from the ground up blending our custom-built OS with secure, durable hardware ensuring only GTL software can function on the device and vice versa.

Inspire Tablets are “Flat” form factor offering a multi-touch screen matrix with an LED backlight. The Tablet is available in 4” and 7” size configurations and features 512 MB memory and 8 GB Flash Memory.
Inmates will not be able to access the interior components such as the motherboard of the device. GTL uses clear cases to distinguish the device from contraband and eliminate the hiding of contraband as well.

**Charging Methods**

Regular charging of *Inspire* tablets is critical to availability of the tablets. Charging can also offer a ready capability for maintaining control of tablets, particularly in the “tablets live in-pod” distribution policy.

GTL’s enhanced services wireless tablet is available with three (3) different charging methods:

**Charging Carts**
- Operated by officers who drop off and pick up tablets.
- Able to hold 40 tablets per cart.
- Each bay is .875”w x 10.5”d x 8.5”h
- Inmates can hand in the *Inspire* tablet for every other night charging which gives VADOC authorized staff an opportunity to check devices for tampering.

**Mounted Charging Stations**
- Wall-mounted stations that inmates charge devices themselves.

**Wall Adapters**
- If wall outlets are available, inmates can use GTL’s clear wall chargers.

*The Inspire tablet cannot be opened by inmates—unlike other tablets with removable batteries which could be used as a power source for a variety of contraband devices such as a tattoo gun.*
Inspire Wireless Tablet Applications

Inspire wireless tablets will connect directly to GTL’s inmate telephone system via the secure wireless network. What this means for VADOC inmates is the transition to the Inspire Wireless Tablet calling platform will be seamless for the majority of who are accustomed to GTL’s traditional inmate phones.

Inmates using Inspire tablets—now able to speak to associates from their living quarters—means more communication with loved ones and more calls available for analysis. VADOC Investigators will be using the same powerful analytical tools they are already using.

Inmate Calling

GTL Inmate Calling Application – GTL’s Inmate Calling application for the Inspire™ tablet integrates fully with the current GTL ITS already in place at VADOC. All of the security features of our traditional inmate telephones are observed and available as part of GTL’s Inspire tablet solution. Inspire tablets are simply a gateway for inmates to access GTL’s proprietary inmate phone platform which is software-based. All the same security is now available from the comfort of their cell.

The Inspire tablets are ready for inmate telephone calls NOW!

More than Just a Phone - GTL’s Inspire™ tablet program provides wireless calling for the VADOC inmate population, however there are opportunities to utilize the full capabilities of the Inspire solution as VADOC facilities become comfortable with the technology. By providing these extended capabilities at VADOC correctional facilities, the Inspire™ tablets can introduce powerful incentives for promoting positive behavior within the inmate population.
GTL provides a powerful suite of applications available on the **Inspire** wireless tablet, including:

**Inmate Messaging**
- GTL Message Link (Inmate Electronic Mail)

**Inmate Operations and Facility Documents**
- GTL Document Link (Inmate & facility information, including PDF documents and specific types of approved free e-books or booklets)
- GTL Request Link (Inmate Information and program requests)
- GTL Grievance Link (Inmate concerns)
- GTL Commissary Link (commissary ordering)

**Educational and Informational Services**
- GTL Education Link, Inmate educational programs using partners and applications that meet the needs and goals of the VA DOC
- GTL Law Library (requested state law information)

**Inmate Entertainment**
- GTL Streaming Music (directly streaming songs to the tablet)
- GTL Games Center (download games from the GTL subscription gateway)
- GTL E-book Link (Delivers literature)

Inmates access all Inspire tablet applications via the “Applications Launcher” home screen. Each application requires inmates to login with their Inmate Identification ID and their PIN.

---

2 Inmate Login
No Camera

Some vendors utilize off-the-self tablets not specifically designed for the correction marketplace that have a camera built in. The GTL tablet is specifically designed for the corrections market to avoid the huge security risks and deficiency found when trying to deploy a non-corrections, off-the-shelf commercial tablet. **GTL's tablet was designed specifically to avoid the security situations that can and will occur on tablets with cameras, such as inappropriate behavior in a private setting.** To ensure a safe environment for all, we encourage the VADOC to mandate that the tablets deployed in your facilities do not contain cameras. GTL's approach to video visitation can be found in the next product category: the GTL FLEX Link In-Pod Kiosk. GTL details how to successfully and securely deliver video visitation to the inmate population.

System Operation

The Inspire™ Wireless Tablet system will connect directly to GTL's ITS, already in place at VADOC facilities, via the secure wireless network. All of the system functions for VADOC authorized personnel will operate with the ITS user software with which VADOC users are already familiar.

ITS Web browser-based user tools will all remain the same including the ITS system dashboard of tools, inmate PIN details, call monitoring and recording, reports, number blocking, etc. All investigative and analytical tools will be the same, but additional investigative opportunities become available: inmates will increase communications with associates when allowed to call from their living quarters.

GTL will continue to store call recordings and call detail records; these are available to authorized VADOC personnel for review and investigation on-line using the GTL ITS user interface.

GTL uses tablet management software to automatically control Inspire™ tablet configuration and distribute updates via the wireless network. The updates are issued in real time; depending on network loading at the time of the update. Tablet updates will be delivered in real-time or very near real-time.

Inspire wireless tablet solutions include a tablet control environment called “Platform Elite”. The offender's purchases, refunds, and transaction history may be viewed on our Platform Elite user software. The Platform Elite user interface is a secure, web-based application accessed on-line at the VADOC facility user station or remotely from a central location. User identification is required from a two-factor authentication procedure containing the username and password of the VADOC authorized user.

GTL is constantly introducing new applications to increase the value of the Inspire™ tablet to both inmates and the VADOC, and full integration maximizes our capability for innovation.
GTL Flex™ Link In-Pod Kiosk

For inmate assistive applications, including our industry leading Video Visitation solution, GTL recommends the correction industry’s most innovative in-pod technology, GTL’s patent-pending Flex™ Link in-pod kiosk. For VADOC, the Flex™ Link in-pod kiosks provide inmates as dynamic multiservice and communication kiosks. The Flex™ Link in-pod kiosks are able to be utilized as both inmate and visitor stations for use with our video visitation application solution.

Flex™ Link In-Pod Kiosk Specifications

GTL is able to offer VADOC our state-of-the-art Flex™ Link inmate in-pod kiosk feature. GTL’s Flex Link in-pod kiosk our latest technology in replacing antiquated pay phone service allowing for unlimited expansion of services to inmates while helping VADOC streamline otherwise inefficient clerical processes. The 10.1-inch touchscreen tablet platform is able to allow VADOC to add new products and services for inmates and staff over time. With GTL’s multi-layered security design, Inmates have no access to the internet or other restricted information and systems.

The Flex Link in-pod kiosk has a fully integrated power backup battery built into the unit. No additional battery backup is required to power the unit if facility power is lost.

GTL’s patent-pending design allows the kiosk to fit in the same footprint and on the same mounting brackets as inmate phones. Similar to inmate phones, GTL’s Flex Link in-pod kiosk enclosure mounts to pedestals and other inmate phone hardware should future hardware expansion be needed and/or required. What’s more, with the Flex Link integrated handset and software, inmate phones easily swap out for Flex in-pod kiosk enclosures—without the need for alterations to the facility structure.

With limited wall space and infrastructure considerations, the Flex Link’s unique design and dramatically smaller footprint allows for future expansion without compromising the facility infrastructure and aesthetics.

VADOC approved content will be available to inmates through the touch screen software interface of the Flex Link In-Pod inmate kiosk.
**Flex Link In-Pod Kiosk Applications**

We urge the VADOC to consider all potential future applications of the In-Pod Kiosks when making any decisions. GTL’s unit is multi-purpose and can provide all of the items below. Do not settle for a unit that may only be able to do one or two functions such as music and commissary.

GTL’s Flex Link In-Pod Kiosk is able to provide the following services:

- GTL Inmate Calling (Using the GTL ITS platform installed at VADOC)
- GTL Visitation Link (Video Visitation)
- GTL Message Link (Secure inmate electronic mail)
- GTL Document Link (Inmate and facility information, including PDF documents and specific types of agency-approved free e-books or booklets)
- GTL Request Link (Inmate Information and program requests)
- GTL Grievance Link (Inmates submit grievances electronically)
- GTL Commissary Link (Commissary ordering)
- GTL Account Link (Trust balance lookup and transaction history)
- GTL Media Link w/ Wired Tablet (MP4 music & media player tablet downloads)

**GTL Wired Tablet Specifications**

GTL Media Link enables VADOC inmates to access approved digital media content to use within VADOC facilities through the secure, corrections-grade wired tablets. Digital media content include the entire music library from the four major music labels, e-books, education, self-help, rehabilitation, and other approved content as deemed acceptable by VADOC. The “wired” tablets are also capable of viewing approved pictures (received through GTL Message Link), video, and other programs and services. The GTL Media Link provides an easy to use and secure service for inmates to receive approved media by purchasing it themselves, or having it purchased by family, friends, or other sources.

Inmate downloads of music to the wired tablet devices are performed by linking the wired tablet with the GTL Flex™ Sync kiosk stations and using the GTL Media Link application. Authorized VADOC personnel can manage the Media Link settings using the GTL Platform Elite interface.

GTL’s wired tablet is rugged, shatter-resistant, and constructed of corrections grade materials such that inmates will not be able to access the interior components including the interior circuitry of the device. GTL uses transparent cases to distinguish the device from contraband. As with other corrections grade electronics, such as TVs, it is critical that any handheld device have a transparent housing so that inmates are unable to hide contraband in their device.
With a non-transparent device, an inmate could hide a knife or other weapons and the correctional officers would never see it.

The color LCD screen for the GTL wired tablet device is 4.3” x 2.5” and has a resolution of 800 x 400.

Our wired tablet comes complete with ear bud headphones. The tablet has a manual on/off switch and volume control shown below along with a 3.5 mm connector (shown above) for use with clear ear bud headphones. Devices are available with up to 32 GB of memory storage.

The wired tablet device is also equipped with an FM radio. Inmates are able to listen to any available FM radio stations with the Radio icon on the UI screen. The touchscreen controls enable the user to select stations and control volume.

**GTL ITS System Overview**

The Virginia DOC currently uses the feature-rich GTL Inmate Telephone System (ITS). Our system’s past performance—meeting or exceeding the functionality and security requirements, call controls, and monitoring that are unique to the VADOC—make continuing with GTL’s ITS an ideal solution for VADOC facilities.

GTL’s ITS is a Web-based, centralized, turnkey system that comes complete with all equipment, hardware, and software—including the telephone network, circuits, recording system, call-control system, telephones, workstations, printers, and associated software.

GTL will continue to provide a seamless combination of hardware, software, service, and training to efficiently meet VADOC’s needs. GTL will continue to support VADOC throughout the term of the contract which includes the same experts that design and build the system to maintain and upgrade the software.

The GTL ITS Solution boasts:

- **Open architecture** for easy interfacing with VADOC’s jail management and/or commissary/inmate trust systems
- **Specialized and highly configurable** call-processing and recording system designed and built for use by correctional facilities.
- **Extensive reporting capabilities** for administrators and investigators.
- **Flexible payment options** for inmates and their families and friends.
- **Easy-to-use Graphical User Interface** and password-protected access.
Our **Dedicated network** securely links your facility to GTL’s off-site data centers and makes all ITS features available to authorized users from anywhere there is an Internet connection.

### GTL ITS System Network

GTL’s unique ITS solution includes not only the physical call-processing hardware, but also the corresponding network hardware and circuits, designed specifically for the needs of each correctional facility. With this true end-to-end solution, GTL is able to transmit data over a packet-switched network to continuously back up all call records to our offsite data centers, stream live calls directly to remote investigators, and access phone company databases for highly detailed call validation of each and every call.

While other companies have tried to use all-internet solutions or adapt PBX machines, the GTL ITS solution truly combines the reliability and reach of the PSTN; the security and high-speed throughput of a dedicated, secure WAN; the ease-of access of the public Internet, and the flexibility of a fully programmable server. It is a point of pride for GTL that the team which designs and builds your ITS is the same team responsible for providing your ongoing support.
Anytime, Anywhere Access

GTL’s hosted ITS solution has a Web-based interface that is accessible to authorized individuals via connection to GTL’s private ITS website.

The GTL ITS provides Anywhere Anytime Access to its powerful, technologically advanced features. Properly authorized users may access the system from an onsite system workstation, VADOC’s on-site PCs, or any off-site PC (desktop or laptop). Compatible smart phones with Internet connection can also access certain ITS features.

After connecting to the private ITS Website, the individual must log into VADOC’s system with a valid user-name and password. Each user’s password links to an assigned Role, defined by VADOC, which dictates exactly which features and functionality are available to that user after login.

All system users are subject to security level assignment. All data are accessible on a “need to know” basis. For example, the ITS database management tools would be available only to those granted permission by VADOC to perform system administrative functions.

Remote access to the system is through a Secure Sockets Layer (SSL) exchange. This is the same security system used by many major financial institutions.

GTL ITS System Equipment

GTL builds the ITS solution to the specifications of each client. GTL scales the original installation for the number of inmate phones supported, the amount of call traffic, and the expected number of simultaneous users.

Scalability: The ITS will meet your needs now and in the future. The original installation is configured for the number of inmate phones supported, the number of workstations, the amount of call traffic, and the expected number of simultaneous users. The system design is modular and expandable. If additional capacity is required, such as new inmate phones or a facility expansion, GTL ITS Solution can easily accommodate this need.

Reliability: The ITS’s consistent reliability is provided through high-quality components, multiple hardware redundancies, network design, data backups, and constant remote monitoring and diagnostics. These features, along with hot-swap capability and flexible design, will virtually eliminate system downtime. The system hardware is one of the most reliable computer telephony chassis available today, with a current uptime of 99.9%.

GTL’s ITS platform provides advanced centralized processing and data storage therefore requires minimal on-site equipment. The majority of on-site system equipment is contained in a utility cabinet.
**Data Storage and Redundancy**

Our Inmate Telephone System platform provides centralized storage of all system and call data at GTL Data Centers; effectively putting GTL’s highly trained service personnel continuously “in the room” with your calling platform and call data. Our Data Centers are secure, climate controlled fortresses that ensure the safekeeping of all of your data and protects your system’s functionality. The GTL inmate calling platform provides redundancy to reduce interruption of service and prevent data loss.

When a competitor’s high profile data center outage and far-reaching security breach rocked the industry, GTL’s longstanding investment in its security infrastructure resulted in another stellar year of performance with zero outages, zero data breaches, and over 18M credit card transactions safely executed.

With recent and historical security breaches that have occurred within the corrections industry, it is critical for agencies and facilities to work with a vendor that places the security of their data as the highest priority. We understand that VADOC corrections facilities demand the highest levels of data security both for user access of data and storage of that data. GTL is dedicated to the protection and reliability of our customers’ data using the latest technology and industry best practices. It is the “peace of mind” that comes with knowing that GTL is able to exceed the data security needs of VADOC that we strive toward.

GTL utilizes hardened co-located facilities to provide a highly resilient, highly available, redundant network capable of handling all of GTL’s voice data and call validation and management requirements in the event that one co-location facility fails while in service.

Our data center facilities are physically separate; located in the states of Texas and Alabama. All GTL data storage facilities are lightning and surge-protected and have UPS units and back-up power generators. The databases housed at each data center update automatically so that each center holds complete and up-to-date information for the various facilities.

Each telephony server connects to a RAID, replicating inmate call recordings in real time across a redundant array of independent disks. GTL redundantly stores all call detail records for on-line access for the term of the contract and recordings for the agreed upon storage period.

---

**GTL Data Center Security**

- Perimeter gated fence with guarded access.
- Level 4 hurricane rated building.
- Centralized badge access ensuring only authorized individuals enter and appropriate employees have access to physical servers.
- 24/7 closed caption television monitoring and recording with centralized system providing access to all live and recorded video feeds.
- Approved escort required to accompany visitors and janitorial staff.
- FM 200 fire protection system
- Dual grid AC power
- Diesel powered backup generators
- UPS protection of all servers
- Firewalls and Wireless Intrusion Prevention Systems to alert and block electronic intrusion.
The system’s databases at GTL Data Centers dynamically update as each call is placed and completed, and as system settings change via authorized staff at the facility.

---

**GTL Best Practices**

All GTL operations, such as business practices; system development, deployment and functionality; and data acquisition, handling and storage are subject to stringent, detailed security policies and procedures.

Our inmate phone systems and deposit service systems are rich with fraud prevention features. We present below only a fraction of the policies and procedures GTL has in place to ensure data security and fraud prevention. If desirable, GTL’s Chief Security Officer will be pleased to set up a meeting with the County for an in-depth review of our security methodologies.

GTL is one of the first organizations in the country with an employee that has been certified by the Payment Card Industry (PCI) Security Standards Council as an Internal Security Assessor (ISA). This ensures that our PCI compliance is held to the highest standard. GTL’s handling of sensitive cardholder data is fully compliant with Payment Card Industry Data Security Standards (PCI-DSS). At the end of 2015, GTL had processed 18 million credit card transactions without a single security breach. As a result of our performance and diligence in achieving all necessary qualifications, GTL is classified by PCI as a Level 1 merchant – the highest and most prestigious PCI security classification. GTL backs its expanding automated payment services profile with the highest degree of data security achievable. GTL maintains electronic money transfer licenses in all 50 states, has comprehensive OFAC and AML/BSA policies in place, and is fully compliant with FinCEN and state money transfer regulations.

---

**GTL ITS Systems Integration**

The GTL ITS can be interfaced with virtually any jail management, commissary, other external system that stores and manages data relevant to the inmate calling platform. Interfaces between the ITS platform and a facility’s other systems can provide:

- Automatic transfer of inmate data (name, housing location, etc.) to the inmate telephone system’s PIN database.
- Automatic funding of inmate Debit calls from commissary/trust accounts.

We have successfully integrated with more systems (jail management, commissary, etc.) than any other vendor. Our program and project implementation teams have handled many large accounts, networking multiple sites and integrating with disparate databases. The key to trouble-free, open systems integration is working directly and harmoniously with your existing and future partners. This kind of inter-system integration sets GTL apart from all other providers through:

- The establishment of one team tasked with ensuring smooth integration
- Integration experience from other account to draw upon when problems arise
- Increased revenues as a result of more payment channels and additional services
- Availability of multiple solutions to meet current and future needs

We can interface the GTL ITS with any system that implements standardized protocols, such as SQL, XML, PCIP, HTTP, FTP, FSTP, 3270, and the like. GTL can also work with standard-based middleware that can provide interfaces to external systems.

GTL has also developed web service functions based upon Service-Oriented Architecture that are platform independent.

GTL ITS User Interface

The robust GTL ITS has a deceptively simple interface that gives authorized users access to its powerful and technologically advanced features. The system’s call trace, call history detail, and other call detail reporting capabilities were developed with direct input from active investigators.

Upon secure login, the ITS Home Page displays numerical and graphical summaries of call data for the facility, including total completed and uncompleted calls, total call revenues, revenue breakdown by call type, and statistics based on call results (the various reasons for call terminations). Statistics for the current day are displayed by default, but users may choose alternate time frames by adjusting entries in the Home Page date fields.

The system can generate more than 1,600 different reports based on parameters defined by the user, all from the Call Detail Reporting screen. The ITS also provides a variety of call statistics, revenue, and user-history reports from the system’s Advanced Reports screen.

The ITS system’s Graphical User Interface is straightforward. The simple design allows facility staff and investigators to use the powerful investigative tools and wide range of administrative features fluently after only minimal training.

Selected ITS Features

- Online Help
- Online Support Chat
- Collect, Debit, and Prepaid Options
- Fully Integrated Debit
- External Payment
- AdvancePay Programs
- Integrated Voice Biometrics (Pass Phrase Verification)
- Three-Way Call Prevention
- Number Management
- Reverse Number Lookup
- User Management
- Call Analyzer
GTL ITS – Access to Past Call Recordings/Data

Investigations often times go back several years and the VADOC will need access to old call recordings and call data that may hold the missing piece to the puzzle in solving an investigation. With the GTL solution, the DOC will continue to have access to all inmate phone data and recordings for at least the last five (5) years.

GTL Cell Phone Detection & Managed Access Solution

By being at the forefront in battling the issues surrounding detection and control of cell phones for the past four years, GTL has developed a unique viewpoint into the contraband cell phone problem. With this being said, GTL is able to recognize that each customer has different needs and requirements and as an impartial entity, GTL is able to provide a solution and a preferred vendor network that fits the unique issues of the VADOC. GTL is able to offer our multi-faceted Cell Phone Detection and Deterrent solution to the VADOC as an optional solution if the VADOC is interested in implementing.

GTL has deployed multiple configurations of our multi-faceted cell phone detection and deterrence solution with 18 sites in California DOC and 3 in Mississippi DOC.

Just seven years ago, technology like cell detection, managed access, and handheld radio frequency scanners were not yet deployed in correctional environments. Cellular technology such as LTE was not available. With GTL, VADOC can be confident that the best and most effective technology will always be available. As a trusted advisor, we can guide VADOC to implement the solution that enables VADOC to stay current with the ever-evolving cellular trends in today’s marketplace.

It is important to remember there is no one solution that solves the contraband cell phone problem. As the partner with the most experience in Managed Access we have found that Managed Access is NOT a “one-size fits all” approach. That is why it is important to approach the problem with a truly multi-faceted solution that includes (1) reporting capabilities of the inmate phone system, (2) cell phone detection devices, and (3) cell phone data extraction and analysis.
**GTL System Inmate Call Level Reporting**

The GTL ITS system is configured to report inmate calling patterns. These patterns enable GTL personnel to pinpoint specific inmate calling levels where inmates with a pattern of higher calling changes to pattern of very low level calling. This pattern can be shown to reveal an inmate that is now using a cell phone to place calls.

**Ferromagnetic Mobile Cell Phone Detection (Cellsense®/CEIA Units)**

GTL is able to provide VADOC with the ability to detect cell phones within your facilities using a ferromagnetic mobile cell detection device. GTL offers a relatively mobile device that detects cell phones from as far as (3) feet away. The device appears like a metal detector but uses different technology to detect cell phones via non-ferrous metals, which greatly reduces the amount of false positives.

The mobile device detects all cell phones even when the unit is turned off. The unit is completely portable so deployment is possible at any place in each VADOC facility.

Mobile Cell Detection Device Features:

- Detects all cell phones and much more.
- Full body scan with single walk by
- Large numbers of prisoners scanned quickly (> 40 inmates/minute)
- Body cavity detection
- Covert screening option

As with all cell phone detection technology, the mobile device does have a limitation that the cell phone must be moving in order to be detected. Therefore the best deployment is one that has the element of surprise and has inmates walk by it such as the cafeteria line, as visitors enter your facility, as officers enter your facility, etc.

**Cellebrite UFED Forensic Units (analysis of contraband cell phones)**

The Cellebrite UFED Forensic System is the ultimate standalone mobile forensic device, ready for use out in the field or in the lab.
The UFED system extracts vital information from 95% of all cellular phones on the market today, including smart-phones and PDA devices (Palm OS, Microsoft, Blackberry, Symbian, iPhone, and Google Android). Simple to use even in the field with no PC required, the UFED can easily store hundreds of phonebooks and content items onto an SD card or USB flash drive.

Cellebrite UFED supports all known cellular device interfaces, including serial, USB, infrared, and Bluetooth. Extractions can then be brought back to the forensic lab for review and verification using the reporting/analysis tool. Cellebrite works exclusively with most major carriers worldwide including Verizon Wireless, AT&T, Sprint/Nextel, T-Mobile, Rogers Wireless, as well as 140 others. This ensures that future devices are supported prior to retail launch.

- **Secure Extraction, Complete Content:** The UFED allows you to extract a wide variety of data types.
- **Reporting Capabilities:** The Cellebrite UFED system comes complete with a user-friendly PC reporting and analysis software application. Concise, easy to analyze report logs can be generated in HTML, XLS, CSV, and XML formats, providing organized printouts for use as a reference and in the courtroom.
- **Proven User-friendly Interface:** The Cellebrite UFED system is extremely user-friendly, with an intuitive interface that has been proven and field-tested for over 11 years with hundreds of thousands of users.

**UFED Physical Pro - Recover hidden and deleted data:** The Cellebrite UFED Physical Pro is an optional add-on module to enhance your existing UFED hardware. The UFED Physical Pro expands your current device capabilities to extract deleted mobile device data, user passwords, file system dumps, and physical extraction from GPS devices.

**Unparalleled Access to Phone Memory:** UFED Physical Pro provides access to data inaccessible by logical methods:

- Phone user lock code
- Deleted data including: deleted call history, text messages, images, phonebook entries and videos
- Access to internal application data
- Phone internal data including: IMSI history, past SIM cards used, past user lock code history
Intelligent software for Deeper Investigations: The memory dump from each phone is a complex data structure. But the UFED Physical Pro software tool makes navigating this data easy.

Having detected the device, and extracted the data, the next and final step is the Analysis of the extracted data. This is where GTL’s best of breed analytical solutions, GTL Data IQ, ingests the extracted data, providing you with a network of actionable intelligence. GTL Data IQ is a data mining tool designed to digest any number of data sources, including those unique to your facility, and provide you with a visual link diagram of the resulting network.

GTL Is the Leading Corrections Managed Access Provider

GTL highly recommends the multi-faceted approach just previously discussed as our experience dictates that this approach works! However, if the VADOC has a strong desire to proceed with Managed Access standalone we respectfully remind the VA DOC that, as the prime contractor, GTL has more deployments and implementations of Managed Access Systems (MAS) than all other providers combined—with deployments for the State of Mississippi and the State of California.

More importantly, this experience and knowledge is resident within GTL and its personnel not our subcontractor. We have learned from each of our deployments valuable insights such as how inmates respond, how officers respond and perhaps most importantly how wireless carriers respond. This knowhow manifests itself in the following competencies:

- Site Surveys – Site surveys are vital, as simple walkthroughs do not suffice to build a MAS System. It is important to survey the cellular footprint of a site in order to know what cellular technologies are deployed, what spectrum these technologies are deployed on, and where commercial carriers’ towers are located. From this information, we can build a layout of a distributed antenna system (DAS) that can efficiently emanate our cellular signals in order to capture contraband cell phones while still limiting impact off-site so as to not affect commercial carriers’ footprint.

- Optimal distributed antennae system deployment – GTL has gone through the pains of all types of antenna deployments. The first MAS deployments featured antennas at a central point of a facility featuring omni-directional high-powered antennas with Radio Frequencies (RF) emanating out in all directions. This approach while the least expensive to implement, is the hardest to control from an RF perspective leading to bleed off-site as well as coverage gaps on-site. GTL also has experience with antennas surrounding an exterior of a site and using directional antennas to shoot RF inwards. Ultimately, these experiences have moved us toward a hybrid solution of internal and external DAS. The solution is both the most cost effective to implement as well as allows for the most efficient coverage patterns.

- Wireless Carrier Agreements – MAS is completely reliant on cellular carrier agreements. GTL has the relationships with carriers such as AT&T/Verizon/etc., to obtain the licenses and lease agreements for the spectrum covering VADOC facilities.
• Wireless Carrier Interoperability - GTL has effectively managed the wireless signals of AT&T, Cricket, US Cellular, C-Spire, Sprint, T-Mobile, and Verizon. This list encompasses the largest carriers operating in the US.

• Suspicious conduct from correctional officers – Unfortunately, GTL has been a victim of MAS equipment being broken by illicit means. This experience has taught us that MAS equipment must be protected and stored in inaccessible places. This must be part of the DAS design otherwise inmates or even officers that have been selling contraband cell phones will proactively seek to destroy MAS equipment. As each piece of equipment is vital to provide a fully functioning system, it is imperative that MAS be properly deployed to avoid these types of expensive repairs that could have been avoided.

• Updates for latest cellular technology such as 4G LTE – Cellular technology is constantly evolving. With our aforementioned experience with the carriers, we have a unique ability to be in-the-know on the latest technologies being deployed. Therefore this allows us to get a head-start on working on integrating technology such as LTE into our MAS. With VoLTE on the horizon, it will be imperative to have a great working relationship with the carriers as well as the technology wherewithal to stay ahead of the curve. As soon as a MAS does not keep up with the latest technology, it becomes significantly less effective as the latest cell phones will be able to defeat the MAS.

• FCC – GTL has successfully passed several FCC inspections. Without FCC support, GTL would not be able to implement MAS. GTL has also been leading the charge with the FCC on the NPRM on MAS. Working hand in hand with the FCC, GTL has been able to facilitate getting experimental spectrum rights in order to put up MAS sites.

• Authorized list – Without a functioning authorized list, MAS would simply be cell phone blocking which is illegal in the US. GTL has led the charge in getting most cellular technology working for authorized phones. As cell phones become more tools for data and less for voice, it is imperative that data functionality is maintained.

• Complexities with one-off issues – MAS is cutting edge technology. As such, nuances to the technology have been identified and fixed by GTL. Examples include dual mode phones (working in CDMA/GSM) as well as contraband cell phones placed in Mylar bags to make a call allowing them to get onto a cellular carrier’s network and not GTL’s MAS. GTL has the knowledge and experience dealing with these ‘one-off’ issues so that VADOC will not have to go through the pain of these types of issues.

---

**GTL’s Commitment to Cell Phone Control**

As evidence of our commitment to a burgeoning industry wide problem, GTL is the only provider to have a full-time dedicated Intelligence Tools Product Manager, Mr. Mitch Volkart, dedicated to contraband cell phones. Prior to GTL, Mitch spent 8 years with the Missouri Department of Corrections as an Investigative Manager. He led the startup of the
Department's intelligence unit of 20 investigators. He was ultimately promoted to the position of Deputy Inspector General.

MAS represent a significant initial and ongoing investment by the prime contractor. GTL has invested millions of dollars in the installation and ongoing maintenance of MAS deployments for our customers. This not only reflects our commitment to address this industry wide problem but our financial capacity to make this investment.

---

**GTL’s Leading MAS Experience and Expertise**

Other than one very small industry provider, we know of no other phone provider with any experience deploying MAS. Additionally, we are the only inmate telephone provider to participate in the *No Cells in Cells* coalition and the only provider asked to participate in the Congressional briefing on this topic.

In our experienced opinion, Managed Access is not the right fit—or the next logical step—for the VADOC. A multi-faceted approach will bring better results and more benefits to your operations.
B.  | Security Features
Virginia Department of Corrections
TOPIC: Security features demonstrating that the device, network, and services are appropriate for use in a correctional setting, along with information detailing that the system contains appropriate IT security features.

**GTL Security Features - Protecting Your Data Is Our Goal**

At GTL, we take information security and data protection very seriously. That’s why we’ve gone to exceptional lengths to safeguard each VADOC’s data and private information that is generated through the course of their relationship with us. Our security architecture provides our VADOCs the reassurance that their data won’t fall into the wrong hands.

It seems like every day a news article is released about data breaches. Hackers, poor security and the use of unencrypted data are just some of the causes of ruptures in the transmission of credit card information. These data breaches result in lawsuits, data being unusable in court, consumer complaints, loss of deposits from a lack of trust in the transmission network, fraud and theft of funds. GTL has taken every necessary precaution to protect consumers and customers from identity theft and inspire trust in its money transmission services.

Unlike several of our competitors, GTL has NEVER had a data security breach of any kind! We can’t stress enough how seriously we take safeguarding YOUR data and call recordings. In fact, GTL is the only inmate telephone vendor with a full time Chief Security Officer (CSO). GTL was the first vendor in the Public Safety Sector to have such a valuable employee that is certified by the PCI Security Standards Council as an Internal Security Assessor (ISA.) In addition, GTL safeguards the Commonwealth of Virginia’s data with policies in place for the Office of Foreign Assets Control (OFAC) and we are Anti-Money Laundering (AML) as well as Bank Secrecy Act (BSA) compliant.

The VADOC wants to do business with a company that treats YOUR data as if it were our OWN highly sensitive personal data. GTL urges the VADOC to require all vendors to fully disclose all security breaches in their past.

**ITS Security Features – Safeguarding Your Inmate Call Data**

**Data Access**

Correctional facilities access their call detail records (CDR) and call recording data through GTL’s facility management system. This web-based, graphic user interface (GUI) requires a username and password for access. Once logged in, each account has an associated Security Level which defines the capabilities of that user. This permits correctional facilities to control employees’ access to data.
Two-factor authentication is required for access to the cardholder data environment (CDE). This means that beyond the use of a username and password, employees attempting to access this environment must also have an Authentication Matrix card that requires them to engage a matrix for challenge and response security questions. This ensures that access to the CDE is still protected even if an authorized employee’s username and password is stolen because the attacker would also need access to the employee’s physical security card.

GTL is always working to improve its Security Architecture, and the following efforts are currently underway to further expand its user access security controls:

- Two-factor authentication for all remote access to GTL networks
- Host integrity checks on all remotely connecting devices to ensure specific security controls are in place on the connecting device
- Two-factor authentication for accessing corporate data

As you and your teams evaluate responses from inmate telephone providers, it is important to understand the importance and priority providers pay to security architecture. The following is a brief summary of GTL’s approach to security architecture. After reviewing our approach, ask yourself, how do other providers approach security architecture? Is it a priority for that company or an afterthought?

**Data Transport**

Consistent with industry best practice, all data stored and retrieved using the GTL Facility Management System is transported using Transport Layer Security (TLS) that encrypts inbound and outbound data during transmission.

**Data Center Electronic Access**

Electronic access to GTL Data Centers is limited exclusively to GTL VADOCs. In addition, controls are in place to limit access only from specific IP addresses. This means that access to VADOC data will be denied if a request is from an unknown IP address.

Furthermore, multiple layers of 128-bit encryption and perimeter firewall protection prevent unauthorized access from the Internet. The encryption of data streams also keeps inmate information, recordings, and VADOC data from being compromised while in transit.

**Data Center Physical Access**

All GTL Data Center access is restricted by a centralized badge system that uses 26-bit access badges. These badges are unmarked to ensure that if one is lost it could not be associated with GTL systems. Only employees are permitted access to GTL Data Centers. Furthermore, administrator access to the badge system is only provided to a select group of employees who are responsible for managing facility and data center access.

In addition to controlled access, all ingress and egress doors at GTL Data Centers are monitored by CCTV cameras that record 24/7 to a centralized DVR management system. The centralized DVR system stores at least three months of recordings of all data centers and
facilities. Cameras are also located in GTL Data Centers to monitor activities inside the data center.

**CDRs and Recordings**

CDRs and call audio recordings are separated and stored on independent and diverse enterprise storage devices. These storage devices only interact with certain servers within the data center. Finally, user names and passwords are used with the storage devices wherever possible.

**Monitoring, Logging, and Scanning**

The GTL Facility Management System Solution tracks and logs all access to the inmate telephone platform, media storage system, and WAN. The firewall that protects the WAN logs any sessions coming through a GTL server, and the networking software logs any user sessions at the application level. This permits management and tracking of all logins. Any login attempts that are not authorized are immediately flagged and checked against the approved user list.

A robust centralized log monitoring solution provides alerts to the GTL Information Security Department based on predefined and internally developed alarm rules. This application is monitored to detect other anomalies that might indicate inappropriate use of GTL assets. Any time a user logs into the system, the system notes the event and the user’s identity in the system’s electronic Log Book. An Audit Log Report is used by GTL to track and investigate user access and record all system changes and activities that take place while each user is logged into the system.

Monthly internal and external vulnerability scanning and annual penetration testing is performed by the GTL Information Security Department and a PCI-approved scanning vendor. Vulnerabilities are promptly remediated based on level of risk. Risk is determined through the use of the Common Vulnerability Scoring System rating and knowledge of the systems. While Payment Card Industry Data Security Standard (PCI-DSS) Compliance requirements only require that GTL perform this testing quarterly, GTL goes the extra mile and performs the testing on a monthly basis.

**Network and Data Security**

All sites are protected by a “stateful” packet inspection firewall. In addition, access control lists (ACLs) limit all inbound and outbound traffic to GTL-specific networks, which include the IP address for GTL Data Centers, GTL web applications, and VADOC-specific network IP addresses.

GTL creates a virtual private network for all facilities, using Internet Protocol Virtual Private Network (IP VPN) technology. All sites are connected to the data centers using 128-bit AES or 3DES encrypted data links so that all validation, call records, and recordings are encrypted when they traverse this network.
Facilities with remote workstations or cellular wireless broadband networks also use IP VPN and are protected by a firewall.

The Internet-facing Facility Management system is only available over a Secure Sockets Layer (SSLv3) to ensure that all traffic is encrypted and meets security best practices. Controls are also available to allow access only to specific IP addresses. This allows control over access to the GTL’s Facility Management system by outside agencies and individuals.

All backup tapes are encrypted before they are sent for off-site storage. It should be noted that PCI only requires that tapes are stored in a “secure location.” Taking the extra step of encrypting the tapes ensures that regardless of its location, the data on the tapes is not accessible to unauthorized persons.

**Credit Card Data**

When GTL stores its most critical information, this data is encrypted at rest using an industry best practice Key Encryption Appliance. The keys used to encrypt the data never leave the appliance, which means that data can only be decrypted programmatically through the use of multiple layers of authentication.

File integrity monitoring is in place on all servers that process, transmit, or store credit card information. This ensures that the GTL Information Security Department is alerted to all unauthorized modifications of critical system files and internally developed software.

NOTE: Selecting a vendor to trust with properly handling the delicate funds transferred from friends and family of your incarcerated population to inmate phone accounts is not one to take lightly. We encourage the VADOC to require all vendors to document security breaches that they or their subcontractors have experienced. Additionally, it is important to understand if providers have been fined for not properly adhering to the law in regards to money transmission and operating without a license. It is important for the VA DOC to know who they are doing business with and what steps they are taking to safeguard all of this sensitive data.

**Virus and Malware Security**

Anti-virus detection is installed on all internal GTL servers and workstations. This anti-virus solution is centrally managed and alerts the Technology Group and GTL’s third-party monitoring company when viruses are detected or security policies are not adhered to.

Intrusion Prevention Systems are deployed to alert the GTL Information Security Department to potential attacks and automatically block such attacks. Many companies choose to rely on an Intrusion Detection System that simply alerts of potential attacks, but GTL’s systems automatically block suspected malicious traffic.

A robust centralized log monitoring solution provides alerts to the GTL Information Security Department based on predefined and internally developed alarm rules. This application is monitored daily to detect other anomalies that might indicate inappropriate use of GTL assets.
**Equipment**

All GTL equipment is hardened to ensure it comports with today’s security best practices. This includes operating system hardening, point-to-point credit card data encryption, application source code auditing, log monitoring, automated patching, anti-virus, and physical security controls.

**Security and Compliancy is our Focus**

GTL is one of the first organizations in the country with employees who have been certified by the Payment Card Industry (PCI) Security Standards Council as Internal Security Assessors (ISA). Recently, GTL achieved the highest level of PCI compliance - Level 1. This ensures that GTL’s system operations security, system access security, and PCI compliance security efforts are held to the highest benchmarks and that PCI security standards are designed into GTL applications and not merely applied ad hoc after the fact. In addition, all GTL employees are required to attend annual security awareness training to reinforce all GTL policies and procedures.

**Inspire™ Tablet Security Features**

Here at GTL we understand that VADOC corrections facilities demand the highest levels of security when implementing new technology. The Inspire™ wireless device line-up was created with the highest level of security using the latest technology and industry best practices. Our goal is to create a “peace of mind” that comes with knowing that GTL is able to exceed the security needs of VADOC.

GTL uses best-in-class security measures to ensure that both the wireless device and the wireless networks are properly protected. With this in mind, we encourage you to examine the strength and safety of the “Five Layers of Security” for our Inspire™ wireless tablet solution; Security, Operating System, Wireless, Network and Application.

**Inspire™ Security Features - Hardware**

GTL has a rugged, shatterproof, corrections grade device which prevents inmates from accessing the interior components such as the motherboard of the device. Inspire™ wireless tablets have a durable clear body to help prevent contraband being hidden in the device. GTL developed the Inspire tablet with many additional security features, keeping VADOC facilities’ safety and security as the highest priority.

- Barrel charger
- Security screws
- Data-only USB port
• No Camera
• No Bluetooth
• No speaker
• No Micro SD card slot
• Non-removable battery

Inspire™ Security Features – Operating System

Our Inspire tablets are custom built by GTL with a secure operating system, offering vastly superior security over product offerings based on stock “off-the-shelf” tablets. GTL built the Inspire tablet from the ground up blending our custom-built OS with secure, durable hardware ensuring only GTL software can function on the hardware and vice versa.

Additional Operating System security features:

• Locked bootloader (no other operating system can be loaded)
• No “settings”
• No factory reset
• No Web browser
• No safe boot
• No wireless tethering

Inspire™ Security Features - Wireless

GTL uses best-in-class security measures to ensure that both the wireless device and the wireless networks are properly protected from malicious behavior. This also provides control to allow only GTL devices onto the network as well as detection of unauthorized devices attempting to access the network and identify ‘rogue’ Wi-Fi networks. If a device is attempting to connect to access an unauthorized Wi-Fi signal the device is detected and disables its wireless connectivity, effectively rendering it unusable.

To further protect the wireless network, GTL has implemented advanced security practices as recommended by the Wi-Fi Alliance through the use of Wi-Fi Protected Access II (WPA2) Enterprise security protocols. All aspects of the wireless network are locked down, thereby limiting an inmate to only approved content.

Wireless Authentication Specifications

• WPA2 with a complex password and MAC filtering.
• Considered best security practices according to Wi-Fi Alliance.
• Inmates do not have access to the setting application so they cannot see another network or change wireless networks via the Inspire tablet.
Wireless Intrusion Prevention (WIPS)

A Wireless Intrusion Prevention System is deployed for all GTL Inspire wireless tablet VADOC facilities to alert and prevent against the installation of rogue wireless access points. This system also ensures that only GTL Inspire tablets have access to GTL wireless networks and cannot connect to any other network.

Inspire™ Security Features – Network

All tablets are registered into GTL’s wireless system during the provisioning process prior to shipping to a facility. The devices specific to the VADOC deployment are loaded into GTL’s network of that facility ensuring that only GTL devices are allowed on the network.

GTL’s devices are designed to only log onto GTL’s wireless network. This process happens automatically upon arrival in the facility and within range of GTL’s access points in a housing unit. GTL can see all the tablets connected to our network and tracks inmates’ use on the network. If another device somehow exists in the area of our network, we can lock the device out of any network through WIPS.

GTL uses an Access Control List (ACLs) with a default deny statement that only allows specifically permitted IP addresses and URLs. The network appliance will then deny all access to the internet with the exception of those URLs or IP addresses that are needed for the tablet and applications to operate effectively.

Inspire™ Security Features – Application

To secure the applications used on the Inspire™ wireless tablet we installed management software which controls all of the tablet software applications. This wireless system application security allows for easy and quick deployment of applications and firmware changed over the air (OTA), without any end user interaction required.

Applications are continuously vetted to confirm that the application content is appropriate for inmates and that no known security bugs exist. GTL’s security staff also checks to ensure inmates cannot communicate via unauthorized means via a tablet such as through leader or comment boards. Additionally, no social media links are embedded within the app.

For VADOC inmates using the Inspire tablet to place inmate phone calls, the inmate will be required to enter his/her PIN in the same way as a call placed using a standard wall-mounted GTL inmate telephone.

GTL’s Inmate Phone Calling application for the Inspire™ tablet is fully integrated to the GTL Inmate Telephone System. ALL calling controls and security controls that are defined by the VADOC will be applied to calls made using the tablet. Tablets are simply a gateway for inmates to access GTL’s proprietary inmate phone platform which is software-based.
All Enhanced Services applications requiring interaction with VADOC staff are in real-time.

GTL’s Inspire™ wireless tablet solution includes a tablet control environment called “Platform Elite.” GTL’s Platform Elite user interface allows central management of users, software applications and inmate tablets. Through the platform it is possible to disable tablets on an individual basis, by location or by facility. Authorized administration users can disable tablets locally or centrally according to their assigned system privileges.

For security reasons, GTL recommends using the Flex Link in-pod kiosk for Video Visitation, rather than the Inspire™ tablets. Video Visitation on in-pod kiosks is more secure than tablets and protects the safety of correctional officers. Again, certain vendors utilize off-the-self tablets not specifically designed for the correction arena that have a camera built in. These companies push to allow video visitation on the tablet to turn this huge security risk and deficiency in their overall tablet program into a positive. We know that this puts the safety and security of the facility and the public at risk. We encourage the VADOC to consider the multitude of issues that could result from video visitation on a tablet (e.g. aid in escape planning, videos ending up in the public, inappropriate behavior).

Inspire™ Security Recap

- **ZERO** security issues
- **ZERO** issues of inmates hiding contraband in the tablet
- **ZERO** issues of inmates using the tablets as weapons
- **ZERO** issues of inmates accessing content that is not permitted outside of GTL’s secured network, such as Facebook

Wired Tablet Security

- **Secure Logon:** A PIN number is used for individual inmates to login with. Only approved inmates can access Media Link.
- **Downloads:** Media purchased and downloaded by an inmate can’t be downloaded for free by another.
- **Tamper Proof Software:** The GTL wired tablet with Flex Sync kiosk solution prevents access to the internet or other unrestricted information and systems.
- **Security from Theft:** Anti-theft feature locks out a media device if it is reported lost or stolen. It is rendered inoperable to anyone other than the rightful owner.
- **Content:** Only approved content from a pre-screened list is available to inmates. Content deemed a security risk or inappropriate will not appear on the list of available choices.
• **Secure Launcher:** Secure home screen takes the place of the standard UI.

![Secure Launcher](image)

- Remotely managed and controlled UI that limits the user to only those applications approved by both the GTL Information Security Department and VADOC.
- Approved applications and content are distributed to wired tablet from a remotely accessible and secure management environment.
- No access to wired tablet settings.
- **Secure Operating System – Device Operation Security:**
  - Locks the OS of the wired tablet device to allow for only the functionality approved by both the GTL Information Security Department and VADOC.
  - Can send messages to inmates via on-line portal.
  - Can lock and wipe device remotely.
C.  | Hardware and Software Updates

Virginia Department of Corrections
TOPIC: The process that your company has for updating hardware and software.

Software updates are installed remotely from the Technical Assistance Center in the GTL Primary Data Center. These updates are performed during low- or no-usage periods (e.g. 00:00 – 07:00). A local technician will be on site during every update to assist in verification and resolution of any issues.

GTL utilizes a Configuration Management plan to guide us through hardware and software updates and upgrades of the ITS system. Below is our Configuration Management plan approach followed by a lifecycle management flow chart.

---

**ITS CONFIGURATION MANAGEMENT PLAN**

GTL’s Configuration Management focuses on establishing and maintaining consistency of the ITS system’s performance and ensuring that its functional and physical attributes are in compliance with VADOC design and operational requirements throughout the term of the Agreement.

**Hardware Configuration Management**

In preparation for the initial implementation of the ITS following contract award and prior to the installation of any hardware components, GTL will submit for VADOC Designee approval pre-installation documentation that includes technical specifications and drawings and/or diagrams of the proposed equipment, installation location, and, if applicable, network connectivity.

In instances where the actual installation deviates from the model system drawings and diagrams, GTL will notify VADOC Operations Manager of the deviation and provide as-built drawings and diagrams that reflect the actual installation.

All installed hardware documentation will be maintained by GTL, and updated as needed for the term of the Agreement. Documentation of installed hardware will be provided to VADOC in hard copy and electronic format as required.

**Planned Hardware Upgrades**

GTL’s Project Manager will review with VADOC Designee reasons for potential hardware upgrades; ensuring that upgrades are in keeping with VADOC goals and requirements for the system as a whole.

At least thirty (30) days prior to the projected date of a planned hardware upgrade, GTL will submit for VADOC Designee approval documentation that identifies the existing equipment to be replaced and technical specifications of the proposed new equipment. Should a hardware upgrade require additions or changes to the existing telephone system infrastructure, drawings or diagrams will be included that show both the original design and the proposed alteration.
Following the upgrade, relevant VADOC Hardware Documentation will be updated as needed to reflect the as-built configuration.

**Installed Software/Firmware Versions**

For the term of the contract, GTL will maintain the following software elements:

- System software standard configurations (settings, releases, and customizations)
- System software maintenance and administration records
- System software upgrades (version releases, patches, hot fixes, et cetera)
- System software procedures and documentation

As with all changes within the inmate telephone system environment, GTL carefully manages the release of new system software/firmware versions. GTL will coordinate all software updates to the ITS with VADOC Designee. Following VADOC approval, software updates install automatically and remotely from GTL’s secure Web Server.

**Security Department Approval:** Any software or firmware changes to security elements (firewalls, et cetera), or features that have the potential to impact system security, are carefully evaluated and must be reviewed and approved by GTL’s Security Department.

Each quarter, every VADOC facility is checked to ensure that all systems and services are operating according to specifications and all software versions are up-to-date. Trained and certified Technical Support Engineers perform every sweep. Sweeps check for things such as software version numbers, storage capacity, module operation, database synchronization and capacity, network health, and function.

The New Release Software Version Control flow chart schematic at the end of this section illustrates our software version control process.

**Planned Software Upgrades**

GTL will coordinate all software updates to the ITS system with VADOC Designee. Following VADOC approval, software updates install automatically and remotely from GTL’s secure Web Server. Our software update policy allows GTL to deliver the highest quality service and support and allows all ITS users to enjoy the very latest enhancements of our platform’s control program – at all times.

Authorized ITS users are notified at their Administrative or Investigative workstations when a new version of the system’s controlling software is available. After login, the authorized user will see a New Release announcement along with a link to Release Notes that introduce and fully explain any new features or enhancements that were developed, tested, and incorporated into the product since the last update.
3 Work Package and Responsibilities Matrix
TOPIC: The ability of the proposed kiosk and/or tablet to allow commissary ordering. The Virginia Department of Corrections currently contracts with Keefe for these services, and the contract expires in July 2017.

**Kiosk & Tablet Commissary Ordering**

With GTL Commissary Link inmates can select and order items to be filled directly by any commissary vendor or the facility. Product images make the electronic store easy to navigate and correctly select the desired items. Purchases through the Inspire™ tablet are automatically deducted from the inmate’s account. Inmate access rules to the commissary application can be applied individually by inmate and by inmate group.

![Commissary Link: Create Order](image)

Should VADOC wish, inmates can use our Commissary Link application to order their commissary from the Inspire tablets while fully respecting ALL restrictions, account balances, etc. within the OMS. Use of phones or the Inspire tablets can replace or supplement commissary ordering.

**FEATURES**

- Browse items by category
- Prices displayed
- View and modify (add/remove) basket prior to commit

**ITS Telephone Commissary Ordering**

GTL is capable and has proven reliability of utilizing our “Commissary Ordering over the Phone” feature. The GTL ITS is able to be configured to provide a speed dial number for inmates to dial into the VADOC facility’s commissary system using the standard GTL inmate
telephones for ordering items or to take advantage of other services provided by the commissary system. We are currently providing similar setups in various accounts within the GTL installed base.

GTL is also able to provide inmates the ability to order phone debit time directly through an inmate phone. This process further streamlines the release process, readily allowing GTL to push funds back to the inmate’s trust account prior to release. This allows VADOC to perform a single and simple release of an inmate regardless of issuing a check, cash, or a release debit card to the inmate upon release. All the funds remaining on the inmate’s debit phone balance are purged and his account automatically deactivated upon release.
E.  Kiosk to OMS Integration

Virginia Department of Corrections
TOPIC: The ability of the kiosk and/or tablet to download information (such as scheduling, medical, grades etc.) from the DOC’s Offender Management System.

In order to automate VADOC systems, and therefore reduce staff manual involvement, GTL is able to provide automated interfaces for inmate services such as PIN transfer and inmate debit fund transfer. These interfaces are implemented with the DOC’s JMS system (CORIS by Xwave), your trust accounting vendor and any other vendor VADOC may use today or in the future.

GTL has an existing relationship with VADOC system partners for integration services. We have multiple interfaces with vendors at VADOC sites. Additionally, we provide a partial listing of our integration experience with nationally recognized vendors in the corrections industry. GTL is able to provide VADOC with the most technically knowledgeable and experienced staff in the industry with proven integrations at some of the largest correctional facilities.

Nationally known Commissary Vendors

- Aramark
- Oasis Commissary
- Trinity
- Keefe Commissary
- Southern Sheriff’s Supply

Nationally known Jail Management Software Providers

- GTL Offender Management System (OMS)
- Xwave (CORIS)
- Motorola
- New World
- Spillman
- Intergraph
- Syscon

Integration between GTL’s Kiosks/Tablets and VADOC systems can provide:

- Automatic transfer of inmate data (PIN, name, facility, housing location, et cetera) to the ITS and kiosk/tablet database.
- Automatic PIN update for inmate status change.
- Automatic Real-Time funding of inmate Debit calls from commissary/trust accounts.
- Automated inmate fund balance.
- Commissary and debit fund deposits.
Integration for PIN Information Transfer

GTL is able to provide VADOC with an interface program that allows the GTL systems to import inmate PIN and demographic data generated by the VADOC jail management system (CORIS). For this project, GTL will provide this interface service at no cost to VADOC.

Integration for Automated PIN and Inmate Information Transfer: With integration between the GTL systems and VADOC JMS application(s), an inmate will be able to begin using the ITS telephones and the kiosks/tablets as soon as they are processed through booking. As well, upon an inmate’s release the PIN is deactivated in near real-time.

GTL ITS-JMS integration allows the automatic establishment and updating of inmate information PIN accounts via information transfer from the JMS, without the need for human intervention.

Integration for Debit Fund Transfer

In addition, GTL is able to provide integration which automates in real-time the transfer of inmate funds from their commissary/trust fund to their GTL Inmate Debit Account. GTL will provide integration with both the DOC’s commissary and trust accounting vendors, at no cost to VADOC.

Integration Capabilities

The key to trouble-free, open systems integration is working directly and harmoniously with VADOC existing and future partners. Integration can be provided for the VADOC systems using real-time XML, as well as any vendor system that implements standardized protocols, such as SQL, PCIP, HTTP, FTP, FSTP, 3270, and the like. GTL can also work with standard-based
middleware that can provide interfaces to external systems. GTL has also developed web service functions that are based upon Service-Oriented Architecture and that are platform independent. GTL’s system architecture is designed to be platform independent and to accommodate advances in investigative techniques. The following illustrates a partial list of the technologies used in the past for completing foreign (third party) system interfaces:

- **XML** – Our preferred transport protocol for information sharing is by utilizing the GJXML subset of the NIEM 1.0-1.1 schema.
- **Web Services** – This type of interface is preferred by GTL.
- Direct Database Access
- Shared File System
- **FTP** – The FTP protocol is sometimes used as an alternative to the shared file system when the file systems may not be on the same network.
- **Batch Export to File** – This approach actually works in conjunction with several others listed here.
- **Watchdog Applications** – GTL has optional “watchdog” applications that can watch ODBC/OLE databases, the file system, FTP sites, and web sites for triggering events.
- **Application Program Interfaces** – GTL uses native Win32 API for a variety of interfaces including interface of biometric equipment and portable data collection units.

### Integrated Technology Solutions Leader

GTL products are designed for complete and seamless integration into holistic solutions. GTL is one of the only companies serving the corrections industry who can integrate all the necessary pieces of complex solutions without having to outsource major portions of projects in order to provide the needed functionality.

- **2,300** facilities with
- **1.7MILLION** inmates
- **800+** counties in
- **50** states and the District of Columbia and Puerto Rico
- **50%** share of inmate telephone service market
- **8,800** video visitation stations managed with more than 4MILLION visits per year
- **16MILLION** automated payment transactions in 2015
- **33** state DOC contracts including
- **12** of the 20 largest state contracts
- **29** county contracts of the 50 largest counties
- **27** years of innovation and value
The VADOC will benefit from complete integration of our complete technology product suite. While we are experts at integration with all of our clients’ systems, we have the only existing integration to the VADOC’s ITS. Among the benefits of the integration is that the following features are available on Day One deployment of the GTL Inspire wireless tablets.

GTL has performed thousands of integration projects over the years.

All controls programmed for existing inmate phone calls will be applied exactly the same to tablet calls, and the tablet call data will be available in the same database for investigative and reporting purposes.

GTL offers seamless integration between the proposed Inspire™ wireless tablet and your existing ITS – NO other vendor can provide these features and functionality:

- **One Single Application for Call Investigations, Research, Export and to manage calling restrictions and rules.**
- **Live monitoring** – Users can monitor **ALL** facility calls through the ITS that take place no matter if they are in progress on a tablet or phone.
- **Call Recording Playback** – Users can select and playback any and all recordings that take place between an inmate and the public no matter if they take place from a tablet or phone.
- **Call Export for Investigative Use and Court** - Users can select and export any and all recordings that take place between an inmate and the public no matter if they take place from a tablet or phone.
- **Call Rules and Restrictions** – Users can maintain all call rules and restrictions for all inmate communication within the existing ITS no matter if the inmate attempts a call from a tablet or from a traditional phone.

*Integrated technology is where GTL is better suited than anyone else in the corrections marketplace, and why we offer the most comprehensive portfolio in the corrections market.*

Our solutions align with recognized corrections best practices, including those aimed at preparing inmates for successful reentry to society and reducing recidivism rates.

The Inspire wireless tablet system will connect directly to the GTL ITS currently installed at VADOC via the secure wireless network. All the system functions for VADOC authorized personnel will operate with the current inmate phone system.

Inmate Phone System web browser-based user tools include the current ITS dashboard tool, inmate PIN details, call monitoring and recording, reports, number blocking, etc. will be available for tablet-placed inmate calls. VADOC Investigators will be using the same powerful analytical tools they are already using, but additional investigative opportunities occur with the increase in calls when inmates are allowed to speak with associates from their living quarters.

VADOC deserves/needs/requires a partner offering the highest level of integration. Without GTL’s level of integration, another vendor’s services may result in:
- Manually entering data across various systems.
- Staff spending more valuable time on these administrative duties – taking away from the focus on Control, Custody, and Care.
F. | Kiosk and Tablet Applications

Virginia Department of Corrections
Inspire™ Wireless Tablet Applications

The GTL Inspire wireless tablet provides a powerful suite of applications that can be deployed on the Inspire tablet. By providing the extensive capabilities of the Inspire inmate tablets, the VADOC can introduce powerful incentives for positive behavior within the inmate population.

GTL was the first to put a tablet with calling capabilities in an inmate’s hand. We have the most experience in deploying secure inmate tablet systems.

The Inspire wireless tablet solution is capable of providing delivery of the following features:

Inmate Calling

With GTL Inmate Calling, VADOC inmates are able to place calls to friends and family using the Inspire wireless tablet touch screen. The Inspire tablet will connect directly to GTL’s ITS via the secure wireless network. The Inspire tablet calling application is fully integrated to the GTL ITS. What this means for VADOC inmates is a seamless transition to the Inspire wireless tablet calling platform for those inmates accustomed to GTL’s traditional inmate phones. VADOC Investigators will be using the same powerful analytical tools they are already using. All of the security features of our traditional inmate telephones are available as part of GTL’s Inspire tablet solution.

Inmate Messaging

- GTL Message Link (Inmate Electronic Mail)

Facility Documents and Inmate Operations

- GTL Document Link (Inmate & facility information, including PDF documents and specific types of facility-approved free e-books or booklets)
- GTL Request Link (Inmate Information and program requests)
- GTL Grievance Link (Inmate concerns)
- GTL Commissary Link (commissary ordering)
- GTL Account Link (Trust balance lookup and transaction history)

Educational and Informational Services

- GTL Education Link (Inmate educational programs)
- GTL Law Library (requested state law information)
Inmate Entertainment

- GTL Streaming Music (directly streaming songs to the tablet)
- GTL Games Center (download games from the GTL subscription gateway)
- GTL E-book Link (Delivers literature)

Inmates access all applications via the “Applications Launcher” home screen. Each application requires the inmate to login with their Inmate Identification ID and their PIN.

Description of Applications

GTL Message Link

GTL Message Link is more than just a secure e-messaging application. Message Link allows one-way and two-way electronic communication between inmates and their friends and family via e-message, photo attachments, and video clips. GTL is also able to provide VADOC the ability for inmates to request to print e-messages and photo attachments. Message Link is a corrections-grade application that allows VADOC to import watch list words and automate the scanning and review process of e-messages – flagging suspect content for additional review.

E-Messages – Message Link is a corrections-grade application that allows VADOC to import watch list words and automate the scanning and review process of e-messages – flagging suspect content for additional review as needed.

Photo Attachments - Message Link allows friends and family to capture and attach photographs to electronic messages. The e-messages and the attached photographs must pass through the e-message scanning process built into the Message Link solution.

Video Attachments - Message Link allows friends and family to record and send short video messages.
GTL Document Link

The Document Link app provides VADOC a way to digitally distribute pertinent and necessary facility documents to inmates. VADOC can easily upload PDF documents to Document Link and configure the software to display rules & regulations handbooks, general instructions, notification, etc. as well as educational information through one easy to use interface.

GTL Request Link

The Request Link app allows inmates to submit requests via the Inspire tablet using a simple to use form. Requests then flow through a configurable workflow and can then be reviewed by the appropriate facility staff. Requests can be tracked, reviewed, and responded to using an easy to interface. Request Link provides the VADOC with a new level of operational
efficiency by digitalizing clerical processes – allowing staff to remain focused on safety and security.

GTL’s Request Link, now available with the Inspire tablet deployment, offers VADOC facilities the ability to electronically collect any and all requests which may include complaints. These requests are transported to the OMS and routed to appropriate facility personnel based upon VADOC’s policies and procedures. Handling complaints has never been so easy. It should also be noted the Inspire tablets will include an Inmate FAQ that will allow inmates to resolve issues themselves.

**GTL Grievance Link**

The Grievance Link app allows the entire grievance process to be automated. All communication and findings related to a grievance are entered into these integrated products along with follow up actions and responses. This again completely removes the use of paper and saves VADOC huge amounts of time and money.

This feature allows the entire grievance process to be automated with the use of your OMS and the Inspire tablets. All communication and findings related to a grievance are entered into these seamlessly integrated products along with follow up actions and responses. This again completely removes the use of paper and saves VADOC huge amounts of time and money.

**GTL Commissary Link**

With GTL Commissary Link inmates can select and order items to be filled directly by the Keefe Commissary Network. Product images make the electronic store easy to navigate and correctly select the desired items. Purchases through the Inspire™ tablet are automatically
deducted from the inmate’s account. Inmate access rules to the commissary application can be applied individually by inmate and by inmate group.

Should VADOC wish, inmates can use our Commissary Link application to order their commissary from the Inspire tablets while fully respecting ALL restrictions, account balances, etc. within the OMS. Use of phones or the Inspire tablets can replace or supplement commissary ordering.

**GTL Account Link**

With GTL Account Link, VADOC inmates are able to access their trust account balances and view all transaction histories on the FLEX in-pod kiosk and handheld tablet.

**GTL Education Link**

GTL Education Link allows inmates to select various educational materials required and approved by the VADOC. Education is a complex product offering, and GTL realizes that one size does not fit all. GTL partners with several educational companies in order to offer education options ranging from adult basic education, vocational education and GED, to life skills education (financial literacy, interviewing etiquette). As with the general consumer market, education costs can vary tremendously. Based on the demographics of the inmate populations as well as budgets, GTL will work with the VADOC to build the best educational suite to address the VADOC’s specific needs. Education will help reduce recidivism, provide inmates a self-paced curriculum, and offers immediate access to educational content.

VADOC may choose from educational options, including:
• Adult Basic Ed/High School Equivalency – GTL’s education blends self-paced learning, practice assessments, and relevant curricula with instruction in Math, Reading, Writing, Science, and Social Studies. Instruction is appropriate for learners at different levels.

• Vocational Education – GTL’s vocational education options includes 20 to 30 of the most in-demand trades. With engaging and informative content, inmates will be better prepared for employment opportunities upon release.

Interactive educational content can be delivered such that the inmate can work on their educational programs in their own space, at their own pace, and at times that fit their schedule. Also, a much wider range of educational offerings can be made available. For instance the following diagram lists different types of education that can be made available.
Not all types will be suitable for each VADOC due to budgetary concerns, length of stay of inmates, current education levels amongst other factors. Therefore it is imperative that GTL and the VADOC work together to build the educational offering that is most impactful and fits the VADOC’s educational goals.

GTL understands that in correctional education, one size does not fit all. VADOC has unique needs and there are a variety of educational content vendors that best meet these needs.

*GTL has taken a vendor-agnostic approach to the Correctional Vendor application—you get to choose!*

**GTL Law Library**

GTL Law Library brings requested state law information to inmates via the tablet touch screen inputs. GTL is working with the preeminent law library vendor to bring their content to the Inspire tablet. As with education suites, costs can vary greatly. GTL will work with VADOC to identify the proper solution based on what type of legal research VADOC wishes to make available.

**GTL Streaming Music**

GTL Streaming Music enables VADOC inmates to access approved streaming music directly to the Inspire tablet. GTL has partnered with a prominent streaming music vendor to build a custom streaming music service specifically for corrections with a library of over a million songs. The streaming music feature is sold in monthly plans to VADOC inmates who can then listen to hours of new, fresh content—keeping inmates occupied. Some competitors have solutions where the inmate purchases the song and then needs to connect their music device to the in-pod kiosk to download said song. This is antiquated technology that is only deployed when a facility will not allow a wireless solution! GTL’s solution does not require the inmate to plug their tablet into the in-pod kiosk to ‘synch’. Most importantly, instead of inmates being forced to listen to the same songs over and over again, streaming music allows them to listen to the newest songs which provides for a happier inmate population.

**GTL Game Applications**

GTL Games Center allows VADOC’s inmates access to corrections-safe games, built by GTL, that are simple yet fun to play. Inmates purchase games through GTL’s custom App Store.

**GTL E-Books**

GTL E-books provides a safe means of delivering literature versus traditional hard-copy books, prevents transport of contraband, increases security, and fosters an environment with readily accessible literature, promoting intellectual discussion among inmates, which helps reduce violence.
Flex™ Link In-Pod Kiosk Applications w/ Wired Tablet Technology

GTL recommends the correction industry’s most innovative in-pod technology, GTL’s patent-pending Flex™ Link in-pod inmate kiosk. For VADOC, the Flex™ Link in-pod kiosks are provided to inmates as dynamic multiservice and communication kiosks. In addition, the Flex™ Link in-pod kiosks are utilized as video visitation kiosks for use with our video visitation application solution.

GTL’s Flex Link In-Pod Kiosk is able to provide the following applications. The descriptions of the applications for Flex Link shown here are the same as those shown for the GTL Inspire wireless tablet.

- GTL Inmate Calling (Using the GTL ITS platform installed at VADOC)
- GTL Message Link (Secure inmate electronic mail)
- GTL Document Link (Inmate and facility information, including PDF documents and specific types of approved free e-books or booklets)
- GTL Request Link (Inmate Information and program requests)
- GTL Grievance Link (Inmates submit grievances electronically)
- GTL Commissary Link (Commissary ordering)
- GTL Account Link (Trust balance lookup and transaction history)

Additional Applications

The following are applications offered only on the Flex Link In-Pod Kiosk:

- GTL Visitation Link (Video Visitation)
- GTL Media Link (MP4 music & media player tablet downloads)

Video Visitation

GTL Visitation Link app couples the best-in-class visitation management solution with GTL’s Flex Link in-pod kiosk to offer a state-of-the-art inmate video visitation solution. VADOC is able to provide to the public an easy to use, efficient mechanism for friends and family to register, schedule, and conduct visitations from their PC or Android device. With enhanced recordings and monitoring capabilities, VADOC staff have complete control over the visitation system at all times – ensuring that visitation policies and procedures are being adhered to and maintained.
GTL also offers a non-Wi-Fi, Wired Tablet solution

GTL Media Link enables VADOC inmates to access approved digital media content to use within VADOC facilities through the secure, corrections-grade wired tablets. Digital media content include the entire music library from the four major music labels, e-books, education, self-help, rehabilitation, and other approved content as deemed acceptable by VADOC. The “wired” tablets are also capable of viewing approved pictures (received through GTL Message Link), video, and other programs and services. The GTL Media Link provides an easy to use and secure service for inmates to receive approved media by purchasing it themselves, or having it purchased by family, friends, or other sources.

Inmates download music to the wired tablet devices by linking the wired tablet with the GTL Flex™ Sync kiosk stations and using the GTL Media Link application. Authorized VADOC personnel can manage the Media Link settings using the GTL Platform Elite interface.

**Music catalog** that contains over 20 million\(^1\) songs that allows inmates to search by genre, artist, song name and album title on the handheld media player. Inmates have unlimited access on their handheld media players to select and then after connecting the player to the GTL Flex™ Sync kiosk station, purchase and download songs which are stored in the local digital media library.

Examples of the many features of the GTL media players:

- Secure login
- Tamper proof software
- Download of approved content only
- Designed for corrections environment

---

\(^1\) Purchasable/Download catalog includes over 23 million songs. Streaming Music library has 1.2 million songs.
Inmates can easily access and store music, video, e-books and photos on supported devices. The GTL wired tablet has an intuitive interface that makes it easier for illiterate or non-English speaking inmates to independently and successfully use available services. VADOC inmates do not have access to the internet. The GTL Platform Elite user interface ‘locks down’ the wired tablet devices and applications ensuring that an inmate cannot ‘break out’ of the application and access any other functions of the tablet or potentially access the internet.

Media

- **Music:** Inmates can search over 20 million\(^2\) songs by genre, artist, song title and album title. Purchased and downloaded music will be stored in the digital media library with unlimited access.
- **E-books:** Inmates can browse through apps and e-books by title and author. The inmate can benefit from self-learning by downloading educational materials.
- **Video/Movies:** Inmates can browse through categories including educational, drama, science fiction and more.
- **Pictures:** Inmates can store approved pictures they have received from family and friends through e-messaging.

Functionality

**Media Library:** Media stored in the library includes songs, videos and pictures. All media downloaded can be organized and accessed through the media library at any time. All purchased and downloaded media is provided to the inmate upon release.

**Media Store:** Inmates have the option of previewing media before purchasing.

**Access to other services:** Inmates may have access to other functions including Message Link.

---

\(^2\) Purchasable/Download catalog includes over 23 million songs. Streaming Music library has 1.2 million songs.
GTL Wired Tablet Security

The GTL wired tablet device will only communicate with the Flex™ Sync kiosk supplied by GTL using the Media Link application with the USB connector found on the Flex Sync Station.

The wired tablet devices cannot communicate with any other MP4 players within the VADOC facility. No tracks/albums or any other information can be transferred between inmate devices. The devices do not support any form of external storage, which prevents any information from being transferred from the media devices.
G. | Financial Models

Virginia Department of Corrections
TOPIC: General pricing information regarding kiosks and related services along with the various different funding models offered by your company.

As the leader in tablet solutions, GTL has found that designing a tablet program/solution for a facility is similar to selecting your new car. What type color would you like, what level of automation would you like in the car, what type of upholstery would you like, what color would you like that upholstery to be, etc. The strength of the GTL tablet solution is that it can be custom designed to meet the needs of the facility, from a financial investment standpoint and the needs of the inmate and the needs of the public. We are more than willing to sit down with VADOC and create a hybrid offer by combining certain offers or create a new offer in partnership. As an example, GTL can offer an ultra-low cost to the inmate for a tablet if the commonwealth assumes Wi-Fi infrastructure costs. If GTL pays for the infrastructure, the tablet cost to the inmate will be higher. Some of the program/solution options include a complete no-cost to VADOC option, a VADOC-administered rental program, or a GTL-administered rental program. We will work with VADOC to determine the most cost-effective solution.

Directly below, we have provided some sample options on deployment. With any of the options described below, at a minimum, GTL expects to see an increase in phone calling. More options can be discussed as well.

**Sample Option 1**
- GTL will provide VADOC with Inspire™ Tablets at NO cost!
- Replacements and Repair for the length of the contract will be at no cost to VADOC!
- NO rental fee associated with the tablets.
- Cost for services on tablets is the highest of the Sample Options.

**Sample Option 2**
- GTL will provide VADOC with Inspire™ Tablets at NO cost!
- Replacements and Repair for the length of the contract will be at no cost to VADOC!
- NO rental fee associated with the tablets.
- VADOC helps to pay for infrastructure.
- Ultra-low cost for services on tablets.

**Sample Option 3**
- GTL will provide VADOC with Inspire™ Tablets at NO cost!
- Replacements and Repair for the length of the contract will be at no cost to VADOC!
- A monthly rental fee will be associated with the tablets.
- Service costs are lower than option 1 but not as low as option 2.

Rest assured at the end of the day the VADOC will have a tablet program that meets everyone’s needs!
H. | Implementation Recommendations

Virginia Department of Corrections
TOPIC: Recommendations to the DOC regarding implementing an inmate electronic communications system that includes inmate telephone services, kiosks, and tablets.

VADOC can count on GTL to walk them through their implementation planning concerns. GTL has vast experience in identifying the most efficient inmate to equipment ratios. GTL can recommend beta site strategies and rollout plans for each facility’s needs. GTL provides certified Project Managers with a unified approach to all aspects of the products and services being delivered. For a project on the scale of VADOC, GTL understands the risks of disparate installation management tracks and wasted or duplicated efforts.

GTL has learned that schedules for implementation of emerging technologies are highly dependent on the specific facility’s physical situation and the services to be deployed. In addition to the traditional corrections telecom considerations such as carrier circuits, there are new considerations such as:

- Locations of Wireless Access Points (WAPs)
- Infrastructure to support WAPs
- Procedures for distribution of tablets
- Services to be deployed on tablets.

GTL offers multiple advantages to the VADOC in that we have familiarity with VADOC facilities and can therefore draw on our detailed knowledge to quickly determine these variables. In addition, due to our established relationships with VADOC personnel, we will be able to rapidly define the specific Tablet services desired for roll-out by the VADOC.

GTL is recommending our Inspire™ tablets and Flex Link In-Pod Kiosks for Video Visitation for VADOC based our knowledge of current security policies, procedures, staffing, and the layout of VADOC facilities as well as the most advantageous financial model. GTL’s Scope of Work includes the following components:

- System Installation
- System Operation
- Maintenance

**System Operation**

The Inspire™ Wireless Tablet system will connect directly to GTL’s inmate telephone system, already in place at VADOC, via the secure wireless network. All of the system functions for VADOC authorized personnel will operate with the Inmate Telephone System user software with which VADOC users are already familiar.

- ITS Web browser-based user tools will all remain the same including the ITS system dashboard of tools, inmate PIN details, call monitoring and recording, reports, number blocking, etc. All investigative and analytical tools will be the same, but additional investigative opportunities are created with more calls available to analyze with inmates speaking to associates from their living quarters.
• Call recordings and call detail records will continue to be stored and made available on-line for use by authorized VADOC personnel for review and investigation using the GTL ITS user interface.
• All of the security features of our traditional inmate telephones are available as part of GTL’s Inspire™ tablet solution. Tablets are simply a gateway for inmates to access GTL’s proprietary inmate phone platform which is software-based.
• The GTL Inmate Telephone System is currently integrated with VADOC’s required vendors including the inmate accounting software. This means that the GTL Inspire™ tablet solution will be a seamless transition not only for inmates at VADOC but also for VADOC staff.

**Tablet Distribution**

The distribution method of the tablets is dependent on the tablet usage policy to be employed by the VADOC. Directly below are some optional methodologies:

- Each tablet is assigned to a specific inmate and is used only by that inmate (“tablet stays with inmate”).
- Each tablet is assigned to a specific pod and can be used by multiple inmates (“tablets live in-pods”).

The usage policy may be determined by the financial model employed. Should tablets be rented to inmates either by GTL or by the VADOC, then the “tablet stays with inmate” policy would be appropriate. However, this response will describe both models below.

**Tablet Stays with Inmate**

Tablets are physically assigned (potentially by a Property or Commissary Officer) and manually assigned to a specific inmate. If the inmate moves to a new area, the tablet will move with him/her. If the inmate is no longer using the tablet (is released, declines to renew rental, etc.), the tablet will be returned to the issuing VADOC authority and it can be assigned to another inmate.

**Tablets Live In-Pod**

GTL can also support a model in which tablets are pooled by housing unit and can be provided as desired (subject to Facility policy) to any inmate. This model provides an advantage in there is no need for any action when inmates are released or move to another area. In addition, this removes the ‘haves and haves not’ politics within a housing unit.

Tablets are maintained in and distributed from charging carts or cabinet. Designated housing unit officer assigns tablets to inmates per VADOC policy. When an inmate is released or moved to another area, the tablet is just returned to the common pool.

GTL does not recommend the deployment of officer tablets with administrative privileges and controls. Any officer carrying a tablet would be at risk for an inmate to employ either coercion or physical force in an effort to overtake the system controls. Administrative control changes should always be made from a secure workstation.
Training

GTL will provide user manuals and onsite and offsite training for VADOC staff and inmates to learn how to use the system and the tablets. Webinars are available for offsite training.

Through past tablet experience, GTL will work with VADOC to formulate the proper policies and procedures around the tablet program. Such policies include, but are not nearly limited to, how tablets are charged, what times inmates can have tablets, or where inmates can take tablets. This is new technology in corrections and without the proper policies around the program, it will not be successful. VADOC can rely on GTL as a trusted partner to build the proper program to make this a success.

Data Analysis

The VADOC generates an unimaginable amount of data every day! DOC investigators need a tool that can help sort through this tangled mess of seemingly unending data. GTL has developed just the data mining tool for the job, Data IQ!

Designed with input from leading investigators, this field-tested technology reveals previously hidden activities with link chart analysis, identifies unusual patterns and helps investigators solve and prevent crimes. Data IQ is a powerful visual link charting application that ingest data from virtually any source and makes sense of vast quantities of data that could have otherwise gone undetected.

Data IQ creates a huge divide between GTL and the competition, as this tool will ingest ALL VADOC data sources – not just GTL data. With GTL, Data IQ is the ONLY data mining tool your investigators will need.

We encourage the DOC to do their own due diligence on all vendors’ investigative tools. GTL has one All-Encompassing investigative tool for your investigative staff, as opposed to our competition that only analyze data produced by their own stand-alone systems. This means your investigators will be searching and jumping between multiple systems and multiple databases, allowing key pieces of the puzzle to potentially slip through the cracks.
I. | Company Information

Virginia Department of Corrections
TOPIC: Information about your company along with contact information of customers currently contracted with your company for both inmate telephones and kiosks and/tablets.

For 27 years, GTL has been the trusted, one-stop source for integrated technology solutions for the corrections market. VADOC has partnered with GTL in providing enhanced communications to VADOC inmates and their loved ones for 24 of those 27 years! It includes the largest continuous network monitoring and management at GTL’s world-class Network Operation Center. It includes the financial capabilities of a reputable and solid investor, American Securities, a leading U.S. middle-market private equity firm that invests in market-leading North American companies with annual revenues generally ranging from $200 million to $2 billion.

GTL has 24+ years of experience with the VADOC! No other competitor or vendor can state that. Through this period of time, GTL has provided continued service through three (3) different DOC Administrations.
Wireless Corrections

Technology has evolved at an exponential pace over the last decade. Correctional institutions face complex decisions on adopting new technology while adhering to their security standards. Simply ignoring the problem is not an answer since a lack of access to technology while incarcerated could ultimately increase recidivism. This is due to inmates reentering an unfamiliar world that requires technical skills and knowledge they may not possess, or due to time spent in custody not spent on rehabilitation.

GTL’s Inspire™ Wireless tablet program is the answer to meet this necessary market need. Through the deployment of corrections grade Wi-Fi networks and devices, GTL will provide access while still providing safety and security protocols demanded by the corrections market. Inspire™ wireless tablets allow GTL to provide new products such as video and music content, games, and other communication products such as instant messaging and secure email messaging.

In addition to our experience and vision, GTL recently invested in nearly 20% more full-time employees to ensure the company continues to meet VADOC’s growing requirements. GTL currently has over 600 employees.

- **Big Picture Visibility for Facilities.** We help correctional departments gain an unprecedented view into virtually every aspect of their inmate populations and facilities. GTL facilitates driving higher levels of control and safety, thus enabling them to meet current and future operational challenges with confidence.
- **Greater Options for Inmates and Families.** We connect inmates with the people and services that contribute to their rehabilitation. Our solutions align with recognized corrections best practices, including those aimed at preparing inmates for successful re-entry to society and reducing recidivism rates.
- **A Better Experience for Everyone.** GTL is committed to providing visionary technology, unmatched VADOC care and exceptional value to every corrections audience.

Emphasis on VADOC Service

GTL is committed to providing the finest level of technical support for VADOC and the very best VADOC service for the families and friends of inmates who use our services. Technical support and billing VADOC service are provided entirely without cost to VADOC.

Our comprehensive approach to service is outlined below.

**Technical Support:** Twenty-four (24) hours a day, three hundred sixty-five (365) days a year, requests for service or reports of malfunctions go directly to GTL’s Technical Service Center where highly trained GTL professionals determine the best course of action. Our toll free technical service number is always answered by a live GTL representative in a U.S. Service Center.
Local Maintenance and Repair: VADOC’s field service technicians provided by and certified by GTL performs on-site repairs and routine maintenance for our installed systems.

Billing VADOC Call Center: GTL provides the public (family and friends of inmates) toll-free access to our knowledgeable VADOC Call Center staff seven days a week, twenty-four hours a day. We provide live VADOC service in both English and Spanish.

GTL has the most experience in providing tablets to the correctional marketplace. The Inspire™ tablets, unlike most other tablets being sold to the corrections marketplace, are manufactured specifically for GTL and are corrections grade! For the past couple of years GTL has been building our tablet solution for corrections based upon our industry leading understanding of corrections along with conducting correctional focus groups to gain additional information on what corrections needs. This approach guarantees the success of our tablets in almost all correctional environments. Based upon this development methodology and GTL’s unparalleled knowledge of VADOC, it is with utmost confidence that we state that this tablet program will definitely be a success at your facilities! No other vendor can provide VADOC with a tablet solution that is fully integrated into your existing ITS system! They may promise to do so, but for GTL the work has already been completed!

As the current provider of the VADOC ITS, GTL is the ONLY company positioned to deploy the Inspire™ Tablet solution—fully integrated with the ITS—allowing immediate use of tablets by VADOC’s inmates. No additional programming or configuring is required which provides a huge savings of both time and money to VADOC.

NO other vendor can provide these features and functionality.

Virginia DOC staff will work with a GTL team comprised of professionals who understand the VADOC through our 24 years providing Inmate Telephone Services for the VADOC. Our team will include the following members:

<table>
<thead>
<tr>
<th>Full Name of GTL Employee</th>
<th>Position for this Contract and Primary Responsibility</th>
<th>Contact Phone Numbers</th>
<th>Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tom Gibney</td>
<td>Account Executive/ Primary Contact</td>
<td>Cell: 814-330-3830</td>
<td><a href="mailto:tom.gibney@gtl.net">tom.gibney@gtl.net</a></td>
</tr>
<tr>
<td>Anthony Pellegrino</td>
<td>Vice President – Mid-Atlantic Sales/ Primary Sales Oversight</td>
<td>Office: 814-515-1760 Cell: 814-330-3832</td>
<td><a href="mailto:anthony.pellegrino@gtl.net">anthony.pellegrino@gtl.net</a></td>
</tr>
<tr>
<td>Tom Zidar</td>
<td>Field Service Manager / Primary Oversight Field Technician and Installation Oversight</td>
<td>Office: 804-674-1536 Cell: 804-221-6809</td>
<td><a href="mailto:tom.zidar@gtl.net">tom.zidar@gtl.net</a></td>
</tr>
</tbody>
</table>
GTL has successfully deployed and maintained an inmate tablet program in the Alameda County Jail for over a year. A video describing this successful program “Total Transformation: The Role of the Inspire Tablet in Alameda County” is available at http://youtu.be/BrB7_Vi5C_4.

References

**Wireless Tablet Reference: Pima County, AZ**

<table>
<thead>
<tr>
<th>Contact Name</th>
<th>Captain Sean T. Stewart, CJE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organization</strong></td>
<td>Corrections Support Division Commander</td>
</tr>
<tr>
<td></td>
<td>Pima County Sheriff’s Department</td>
</tr>
<tr>
<td></td>
<td>Corrections Bureau</td>
</tr>
<tr>
<td><strong>Contact Address</strong></td>
<td>1270 W Silverlake Rd, Tucson, AZ 85713</td>
</tr>
<tr>
<td><strong>Contact Telephone</strong></td>
<td>520-351-8384</td>
</tr>
<tr>
<td><strong>Contact Email</strong></td>
<td><a href="mailto:sean.stewart@sheriff.pima.gov">sean.stewart@sheriff.pima.gov</a></td>
</tr>
<tr>
<td><strong>Description of Services</strong></td>
<td>ICMv, VVS, DataIQ, and Tablets</td>
</tr>
<tr>
<td><strong>Date of Services</strong></td>
<td>Customer since 2009.</td>
</tr>
</tbody>
</table>
### Wireless Tablet Reference: Alameda County, CA

<table>
<thead>
<tr>
<th>Contact Name</th>
<th>Sgt. Dan Dixon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>Alameda County Sheriff</td>
</tr>
<tr>
<td>Contact Address</td>
<td>1401 Lakeside Drive, Suite 1200, Oakland, CA 94612</td>
</tr>
<tr>
<td>Contact Telephone</td>
<td>(510) 272-6878</td>
</tr>
<tr>
<td>Contact Email</td>
<td><a href="mailto:ddixon@acgov.org">ddixon@acgov.org</a></td>
</tr>
<tr>
<td>Description of Services</td>
<td>Inspire™ Inmate Tablets for wireless inmate telephone calling, music, e-books, handbook, education, programming, and calculator. Wireless calling with Tablets using secure GTL calling platform. Inmate telephone services including integrated inmate debit calling, prepaid, and collect calling options for family and friends. Investigative solutions including key word search.</td>
</tr>
</tbody>
</table>
| Date of Services   | 2008 - present Inmate Telephone Services  
                      2014 - present Tablets |

### ITS Reference: Ohio DRC

<table>
<thead>
<tr>
<th>Contact Name</th>
<th>Randy Booth, IT Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>Ohio Department of Rehabilitations and Corrections</td>
</tr>
<tr>
<td>Contact Address</td>
<td>Central Office</td>
</tr>
<tr>
<td></td>
<td>770 West Broad Street, Columbus, Ohio 43222</td>
</tr>
<tr>
<td>Contact Telephone</td>
<td>(614) 728-1100</td>
</tr>
<tr>
<td>Contact Email</td>
<td><a href="mailto:randy.booth@odrc.state.oh.us">randy.booth@odrc.state.oh.us</a></td>
</tr>
<tr>
<td>Description of Services</td>
<td>ADP of 51,500—and an average of 1.3M calls completed each month. The Ohio DRC currently has approximately 2,690 inmate telephones as well as video visitation, deposit kiosks and intelligence services.</td>
</tr>
<tr>
<td><strong>Flex Link In-Pod Kiosk Reference: South Carolina DOC</strong></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Contact Name</strong></td>
<td>Tom Barrett, Assistant Division Director, Division of Resource &amp; Information Management</td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td>South Carolina Department of Corrections</td>
</tr>
<tr>
<td><strong>Contact Address</strong></td>
<td>4444 Broad River Road, Columbia, SC 29210</td>
</tr>
<tr>
<td><strong>Contact Telephone</strong></td>
<td>(803) 896-1755</td>
</tr>
<tr>
<td><strong>Contact Email</strong></td>
<td><a href="mailto:barrett.tom@doc.sc.gov">barrett.tom@doc.sc.gov</a></td>
</tr>
<tr>
<td><strong>Description of Services</strong></td>
<td>GTL provides South Carolina DOC’s centralized <strong>Focus</strong> Inmate Telephone System for automatic call control and system management, digital recordings, live and remote monitoring and reporting for collect, pre-paid and debit calls to inmate families and friends. Service provided by the centralized <strong>Focus</strong> system configuration. We are providing in-pod kiosk, electronic messaging, inmate banking and commissary services as well. GTL provides the DOC with 6 site administrators and 4 field service technicians located throughout the State. GTL utilizes an MBE to provide these services.</td>
</tr>
<tr>
<td><strong>Date of Services</strong></td>
<td>Current Contract: May 7, 2011.</td>
</tr>
</tbody>
</table>
March 28, 2016

Peter Batley, VCO, CPPB, Procurement Manager:

On behalf of the CenturyLink Public Communications, Inc. (“CenturyLink”) account team, we welcome the opportunity to respond to the Request for Information (RFI) for Inmate Electronic Communication Systems for the Department of Corrections (“DOC”). CenturyLink is confident that our response to the DOC’s RFI will help the DOC identify the current state of technology and services available from CenturyLink. Our Senior Account Manager, Victoria Johnson (859.734.9424), will be your primary contact for any questions on our response that you may have.

CenturyLink has over 25 years of Inmate Electronic Communication Systems implementation and support experience. Further, we believe our combination of in-state presence, financial resources, customer service, technical expertise, in-depth operational experience, and qualified personnel are unmatched in the industry. We currently provide inmate communication services for approximately 310,000 inmates nationwide, including nine state departments of corrections.

*CenturyLink has a consistent and documented history of meeting and exceeding every contractual requirement; time after time we have proven our flexibility by implementing new services beyond the scope of the original proposal and subsequent contract. We encourage the DOC to call any of our current or previous accounts to verify this and we strongly urge that you compare our references to those from the other bidders.*

At CenturyLink, we believe that a product is only as good as the people standing behind it. Our fully staffed support center is always on call, and our entire staff is dedicated to providing the best customer support in our industry.

Sincerely,

Paul Cooper, Vice President and General Manager
CenturyLink
CenturyLink is pleased to submit a response to Virginia Department of Corrections ("DOC") RFI DOC for Inmate Electronic Systems.

CenturyLink is a leader in inmate communications technology and has extensive experience serving state Departments of Correction. We confidently state that by partnering with us, the DOC will receive the most state-of-the-art inmate communication systems, increasing safety for the public, staff, and inmates.

We are committed to being a true partner and align with the State to deliver best-in-class technology and work collaboratively with other technology partners of the DOC.

CenturyLink Public Communications, Inc. ("CenturyLink") has been providing best-in-class services to correctional facilities for over 25 years, connecting inmates with their families while providing the highest level of security to correctional staff and the public. During this time, CenturyLink has a demonstrated track record of exceptional service to correctional facilities nationwide.

As part of a network and managed service provider, CenturyLink is also uniquely positioned in the Corrections Industry. While recent trends in the industry include growth in video visitation solutions, delivering content to tablets, and other bandwidth intensive products, these types of solutions will quickly bring any network problems to the attention of a facility.

CenturyLink understands these network demands and has the assets and expertise to engineer network solutions that alleviate service issues for our customers.
In recent years, we have continued to emphasize a couple of key differentiators that are the pillars of our success. First, we embrace a partner model where CenturyLink has the flexibility and integration experience to bring customized, best in class, technology solutions to the facilities we serve.

Second, in an industry where the word “service” often times has a hollow meaning, CenturyLink prides itself on service that truly differentiates us from our competition in our approach to how we meet the needs of facilities as well as inmates, friends & families. This dedication to service has benefited us well as CenturyLink is now the fastest growing company in the inmate telephone systems (ITS) industry when measured on additional inmates served. Within the last two years, we have successfully transitioned four new State DOC contracts including Utah, Arizona, Idaho and West Virginia, in addition to securing new long-term contracts with Kansas and Nevada DOCs.

While we take pride in this growth story, the retention of our existing customers is a better testament to the CenturyLink approach, service model, and the customer centric product development of the ITS platform. CenturyLink has only lost one customer from the proposed ITS solution – a small county facility - since our first installation with this technology nearly ten years ago. This is a story where we take great pride and appreciate the customer loyalty over the last decade.

CenturyLink Technology Assets & Capabilities

Inmate communications involve managed IT services requiring a broad range of technical, financial, and service capabilities, and no company is positioned as well as CenturyLink to successfully integrate the ITS with any other systems now or in the future.
The capabilities of CenturyLink Public Communications, Inc. coupled with the extensive corporate resources of parent company, CenturyLink, Inc., allow us to provide end-to-end technology solutions that others in the industry simply can’t duplicate. As a leading network and IT provider some of the capabilities and resources that set us apart are:

- Nationwide 250,000 mile fiber optic network
- 56 class 3 and 4 data centers
- One of two commercial service providers authorized by Department of Homeland Security to provide Enhanced Cybersecurity Services
- Cloud and collocation services
- Full portfolio of managed services including voice, data, hosting, and security
- Big data and advanced analytics solutions

The Inmate Electronics Communication Solution & Technology

The proposed IECS centralized platform is a state of the art system that is browser based with anytime/anywhere access, has an intuitive user interface, and boasts an extensive list of product features that are fully integrated into the platform.

This emphasis on integration is critical, and the IECS has a broad feature set fully integrated in the platform to ensure usability for DOC users today AND the ability to add additional functionality as future needs arise. Investigative tools such as link analysis, keyword search, voice biometrics, and our enhanced call player are all inherent in the platform and are not separate “modules” cobbled together from third party acquisitions, nor do they require installation of software supplements. In addition, CenturyLink has extensive technology partners to bring additional services to DOC that were not specifically requested in this RFI. The following table provides a brief summary of technology and services available to the State.
## CenturyLink Solution At A Glance

### System Features

- ✓ Multi-layer redundancy *Industry Leading*
- ✓ Browser-based Easy to Use Interface
- ✓ Online Reporting Capabilities
- ✓ Remote Access
- ✓ Integrated TDD *Industry Leading*
- ✓ Centralized Call Processing
- ✓ Lifetime Online Storage of CDRs
- ✓ Extensive Call Controls

### Service Features

- ✓ Lifetime Repair & Warranty
- ✓ Inmate/resident & Called Party Training
- ✓ Free Software Upgrades
- ✓ 24 x 7 x 365 Technical Service
- ✓ Ongoing Staff Training
- ✓ Inmate/resident & Called Party Instruction

### Calling Services

- ✓ Collect, Prepaid Collect & Debit Calling Programs *Industry Leading*
- ✓ Custom Call Prompts & Voice Overlays
- ✓ Automated PIN/PAN and other OMS data interfaces
- ✓ Self-Learning PAN Capability
- ✓ Multiple Language Prompts – additional languages at no cost
- ✓ Inbound inmate voice messaging

### Facility Operational Tools

- ✓ “The Communicator” Voice-Verified inmate communications portal, including staff-to-inmate messaging and appointment scheduling *Industry Leading*
- ✓ Emergency auto-dial service to family members
- ✓ Integration with other DOC systems, always at no cost
- ✓ Voice-Verified Information Line, including account balance and other confidential information *Industry Leading*
- ✓ “The Attendant” Interactive Voice Response system for automated responses to family inquiries
- ✓ Phone-based commissary ordering

### Fraud Controls

- ✓ Three-Way Detection *Industry Leading*
- ✓ Call Forward Detection *Industry Leading*
- ✓ Hook Switch & Secondary Dial Tone Prevention
- ✓ Chain Dialing Prevention
- ✓ Inmate/resident-to-Inmate/resident Communications Detection *Industry Leading*
- ✓ Incoming Call Block
- ✓ Real-Time Call Validation
- ✓ Extra Dialed Digit Prevention
- ✓ Global and inmate-specific number blocking
### Investigative Tools

- Unlimited Reverse Directory with Satellite Mapping  
  "Industry Leading"  
- 4-channel Audio Separation – Critical for Voice Biometrics & Word Search  "Industry Leading"  
- Unlimited Billing Name and Address Lookup  
- Frequently Called Number Reports  
- 100% Monitoring & Recording of Non-Confidential Calls  
- Data Mining & Link Analysis  
- Voice Biometrics (Pre-call validation included in offer)  "Industry Leading"  
- Funding Alerts  "Industry Leading"  
- Crime Tip & PREA Lines  
- Access to CenturyLink Carrier Database information  
- Call Alerts  
- Barge In Capability & Call Forwarding to Investigators  

### Value Added Services*

- Phone-Based Commissary Ordering  
- Inmate/resident Medical Scheduling  
- Edovo Education & Entertainment Tablets Detection  
- Location Data Services (LocAid)  
- Continuous Voice Biometrics  
- Word Detective (Keyword Search)  
- Contraband Cellular Solutions  
- Inmate/resident-to-Inmate/resident Call  
- CRIMES Data Mining & Investigation  

**Broad Offering of Value Added Services Above and Beyond Basic Inmate/resident Telephone Services**

---

**CenturyLink & Keefe**

As referenced earlier, CenturyLink’s success in the marketplace is driven by our model of building key strategic partners to bring best-in-class technology solutions. In our response, the tablet and kiosk section is leveraging our partnership with Keefe Commissary Network, L.L.C. (Keefe), a division of the Keefe Group. Keefe has been serving the corrections industry since 1974 and has become the leading manufacturer and distributor to the correctional market. Keefe offers technology solutions that increase efficiency and security for correctional facilities. Keefe is leading the way on several fronts, streamlining the way the industry manages and processes inmate commissary, the flow of information, financial transactions, and inmate entertainment and education via our handheld media program.

Keefe’s Handheld Media Program is the only proven correctional Media program currently operating in 16 state-wide DOC’s as well as the Federal Bureau of Prisons. Keefe serves over 525,000 inmates and has delivered tens of millions of songs. The solution includes the option of Secure Mail/Photo Electronic Messaging program, allowing inmates to receive and respond to electronic messages/photos.

Because song catalogs are pre-loaded on the players, inmates are able to browse for songs and make their purchasing decisions right from the player – they do not have to be tethered to a
kiosk to shop. The player catalog provides a description of the song, album and artist to insure inmates are selecting the song they want to buy. Inmates will also be able to read and compose email messages directly on the player away from the kiosk.

Education is also an important aspect of the handheld media program. The Education component focuses on two areas: GED prep and Re-entry programs. The Educational program is benefitting from the input and consultation of Steve Steurer, former Executive Director of Correctional Education Association. The goal of the program is to provide DOCs’ educational departments with technology & content solutions that complement current efforts to educate inmates and prepare them for reentry.

The CenturyLink Difference

We recognize that many of the vendor responses and proposed solutions will appear very similar. And as most any Inmate/resident Telephone System users know, despite all the salesmanship, claims of exclusive patents, and focus on features, over 97% of all functions are the same. Call restrictions, link analysis, reporting, even voice biometrics, cell phone detection, and location services are features any top-tier provider, including CenturyLink, can provide.

But the differences show up “around the edges” when real money has to be spent in order to provide a total package:

- Features developed from the ground up directly within the system; no separate “modules” cobbled together from acquisitions
- 4-channel audio separation – critical for word search and voice biometrics
- Network capacity, scalability, and redundancy
- Consumer service model – industry leader by far and critical for regulatory compliance
- Proven willingness to work with any 3rd party vendor
- Carrier database access (to aid in investigation)
- Dedicated and proven service, support and account management to support DOC

In closing, the corrections industry continues to be a very important focus in our business and we are excited about the opportunity to work with DOC. We also understand that some items that are vital to our success, such as, ethics and service are difficult to score during an evaluation. With that said, we urge DOC to call any of our accounts to learn more about our service model and our commitment to our customers.
1. **PURPOSE:**
   The Virginia DOC of Corrections (DOC) is issuing this Request for Information (RFI) to determine what is currently in the marketplace for inmate telephones, kiosks, and managed access systems.

   This RFI is being issued solely for the purpose of gathering information. This is not a solicitation to purchase goods or services, and no contract will be made as a result of this RFI. The VADOC may or may not choose to issue a solicitation to contract for these items, and the VADOC may or may not choose to incorporate information gathered through this RFI into possible future requirements.

   CenturyLink Response: Read and understood.

2. **STATEMENT OF NEEDS:**
   The intent of this RFI is to obtain information from firms marketing inmate telephone services, kiosks, and managed access systems. The DOC would like to have a contractor install a separate IT network that would enable DOC offenders to place telephone calls and also enable offenders to use correctional kiosks and/or tablets for services such as scheduling, banking, video visitation, secure messaging, learning, training, music, movies, and other related services.

   The DOC would like to utilize a percentage of the communication solution to deliver shared applications and other educational content to offenders within the facilities educational departments. The DOC additionally is interested in learning about the latest innovations in managed access services, to include mobile and fixed solutions which allow facilities to detect contraband cell phones and disable cellular transmissions from such phones.

   CenturyLink Response: Read and understood.

3. **RESPONSES:**
   Interested firms are encouraged to submit an electronic response to this RFI together with marketing materials, a detailed description of the product(s), software, services and capabilities available, and any comments regarding the request listed above, describing what is currently available in the marketplace for inmate telephones, kiosks, offender IT networks, and managed access services.

   CenturyLink Response: Read and understood.

   Responses should be submitted in either MS Word or PDF format that allows key word searches, and responses should include information regarding:

   CenturyLink Response: Read and understood.
A. Technical specifications and features of the inmate phone system, kiosks, IT network and related services, along with technical specifications of the managed access system.

CenturyLink Response: Read and understood.

**Enforcer Inmate Telephone System**

The centralized Enforcer inmate telephone system (ITS) comes with an array of standard features that promote security and efficiency at our clients’ facilities:

<table>
<thead>
<tr>
<th>System Features/Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Remote Access</strong></td>
</tr>
<tr>
<td>The Enforcer is operated through a browser-based GUI (Graphical User Interface). Anyone with a login and password can securely access the system from any computer with internet access and a modern browser as if they were opening a website.</td>
</tr>
<tr>
<td><strong>Easy to Use Web Interface</strong></td>
</tr>
<tr>
<td>The Enforcer's web interface is intuitive, easy to use and functions like any other website.</td>
</tr>
<tr>
<td><strong>Centralized Call Processing</strong></td>
</tr>
</tbody>
</table>
| Call processing occurs on servers running in our secure data centers – leaving a much smaller footprint for equipment installed and maintained at your facilities. In addition to guaranteeing always-up service and high-quality calls, centralized call processing provides several benefits to the DOC, including:  
  ✓ Less equipment at your facilities  
  ✓ Reduced energy consumption  
  ✓ Less onsite installation and maintenance work  

As a result, you will enjoy better performance, more space, cost savings, less onsite disruption, and higher facility security. |
| **Unparalleled Redundancy**                           |
| No other vendor provides as much redundancy for both system operations and data storage.  
  Network Redundancy: For each supported facility, CenturyLink obtains service from two different network carriers, so that if one carrier experiences an outage, service will instantly fail over to the second carrier.  
  **Call Processing Redundancy**: While the primary call processor is housed in our national headquarters and engineering center in San Antonio, we also install a fully functional, always-on backup call processor nearly in Atlanta. Therefore, if a disaster should ever disrupt call processing in San Antonio, service would instantly fail over to the secondary processor in Atlanta.  
  **Storage Redundancy**: Call data and recordings are stored digitally on internally redundant storage devices for the entire contract duration, in two separate geographic locations (one data center in
| **Lifetime Online Storage of Call Data & Recordings** | CenturyLink will securely store all call data and recordings in fully redundant, geographically separate data centers to protect the DOC from any potential data loss. Call data and recordings will be available online for the life of the contract! |
| **Unlimited Expansion Capabilities** | The Enforcer has unlimited expansion capabilities and will be able to accommodate any new construction or future growth of your facility, at no cost the DOC! CenturyLink can add storage and phones at any time without affecting the operations of the existing system. Additional network capacity requires 30 days’ notice for the LEC to hang new lines and does not require any system downtime. |
| **Onsite Reporting Capabilities** | The Enforcer system provides centralized reporting capabilities, allowing facility users to generate reports immediately and in real time. The system comes preconfigured with an extensive list of standard reports. Additionally, a facility user can generate real-time “ad hoc” reports by defining his/her own query based on data of interest – allowing instant access to any report you could ever need. And, although it’s easy to define your own report parameters in the Enforcer, CenturyLink is happy to assist by creating any new, customized reports that are desired. |
| **Hardened Corrections-Suitable Equipment** | CenturyLink has been providing correctional facilities with inmate telephone systems for more than 25 years. All onsite equipment is hardened and tested for use in correctional facilities. |
| **TDD Equipment Compatibility with Transcription Service** | CenturyLink provides our facilities with the Supercom 4400 TDD/TTY unit. The unit itself is compact, lightweight, portable and easy to use. Further, each TDD/TTY call is recorded by the Enforcer and converted to text, which is inserted into a Note and attached to the call recording. Recordings can be accessed from the Call Detail Screen, and attached Notes can be printed locally or remotely by users with appropriate security credentials. |
| **Remote Information Sharing** | If the DOC desires, CenturyLink can provide the DOC with an easy way to share information with other law enforcement and corrections agencies. Because the Enforcer provides flexible and convenient remote access for investigators, multiple investigators can access the system at the same time without impacting on-going system operations or performance. The DOC may grant other law enforcement agencies limited access to inmate information for cooperative investigations. |
| **Service Features** | CenturyLink’s warranty ensures that any and all defective components will be replaced at no cost to the DOC throughout the life of the contract. |

San Antonio and one data center in Atlanta. This storage redundancy ensures that, even if a disaster were to completely destroy one data center, one additional copy of all data and call recordings would still be available for disaster recovery purposes.
<table>
<thead>
<tr>
<th>24 x 7 x 365 Technical Service</th>
<th>CenturyLink’s Technical Services Center (TSC) operates 24 hours per day, 365 days per year in support of our customer sites. When calling our toll free number (866-228-4031) you will be connected with a live, U.S.-based Level 1 TSC technician within 20 seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 x 7 x 365 Customer Service</td>
<td>CenturyLink’s live customer service is available 24 hours per day, 365 days per year. Through our toll-free call center, customers will be connected to our knowledgeable customer service representatives who can help with billing questions, account setup, account status, payments and more. Our customer service representatives can offer multi-lingual assistance including both English and Spanish. All of our customer service representatives are U.S. - based.</td>
</tr>
<tr>
<td>Ongoing Staff Training &amp; Online System Documentation</td>
<td>CenturyLink provides a customized hands-on training curriculum for each facility that we serve. Initial classes are conducted on-site for multiple user groups. We also provide ongoing refresher and new employee training throughout the life of the contract. Follow-up training is typically delivered once per quarter (but can be customized to meet the Facility's needs), and can be delivered live or over the web. Additionally, all system documentation, including User Manuals, Quick Reference Guides, etc., is provided online as part of the Enforcer system.</td>
</tr>
<tr>
<td>Inmate and Called Party Instruction</td>
<td>CenturyLink provides informational pamphlets to the inmates and called parties, which explain how calls are placed and how to open accounts. These pamphlets will be provided to the DOC as requested, at no cost. The most detailed instructions describing the use and functions of the inmate telephones will be provided to DOC inmates via the phones themselves, using the customizable automated operator prompts. CenturyLink also typically provides bilingual (English/Spanish) written instructions in a vandal-resistant display area on the face of each telephone instrument, and we can provide bilingual instructional posters upon request. Called parties can also contact our Customer Service Department or log onto our website at any time to learn how calls are placed and paid for, and how to open accounts.</td>
</tr>
<tr>
<td>Free Software Upgrades</td>
<td>Free, regular software updates are provided at no cost throughout the life of the contract. Whenever an upgrade and/or enhancements to the Enforcer finishes testing and is ready for wide release, the Division will be notified of the new release updates and provided documentation of the features and functions of the new software. New software releases and enhancements are distributed through an IP connection, with no need for any onsite disruption. Enhancements and upgrades to the Enforcer are predominantly driven by market demand and specific client requests. Typically, large upgrades are released quarterly.</td>
</tr>
<tr>
<td>The Communicator℠ 100% Paperless Inmate Communications Portal</td>
<td>The Communicator℠ completely eliminates the need for the DOC to handle and process paper kites. With our paperless process, inmates can file grievances, request medical/dental appointments, submit PREA or crime tip reports, or even file complaints about the Inmate Telephone System – all using secure voice mailboxes on any standard inmate telephone. Depending upon the type of inmate report, the appropriate Facility staff will be automatically notified.</td>
</tr>
</tbody>
</table>
### Response to RFI

| **The Attendant℠ Automated Information Line** | CenturyLink can implement an Interactive Voice Response (IVR) system to provide public and inmate callers with automated information. This can include basic jail information (location, visitation hours, etc.) and, with a OMS integration, inmate-specific information (inmate lookup, release dates, upcoming court dates, bond inquiries, etc.). This inmate lookup feature is available at no cost to the DOC, if the DOC’s OMS will support the data exchange necessary. |
| **Message of the Day℠** | Using the same messaging service developed for The Communicator℠, authorized Facility staff can create a “Message of the Day” that is delivered to inmates via inmate phone during a specified time period. Facility staff can type the message into the Enforcer, and the message is translated to a voice recording using text-to-speech technology; or staff can use traditional voice recording to record their message. They then enter the time window (start/stop dates and times) during which the message will be played to inmates. Any time an inmate picks up any inmate phone during the designated timeframe, he or she will hear the Message of the Day before call connection. When the message expires, it is no longer played to inmates, with no further action necessary from Facility staff. The Facility can use the Message of the Day feature to share information with inmates facility-wide. Additionally, with the Facility’s permission, CenturyLink can create messages to inform inmates of new product rollouts, Facility-approved rate modifications, or other changes to inmate calling services. |
| **Collect, Prepaid Collect & Debit Calling Options** | CenturyLink will offer the DOC inmate more ways to complete calls with our easy to use prepaid calling options. In addition to traditional Collect calling, CenturyLink also offers our facilities:  
- **Point of Sale Prepaid Collect (PSPC℠)** - PSPC℠ allows friends and family of inmates with numbers that are traditionally blocked from receiving collect calls (cell phones, business lines, etc.) to set up an account and prepay for inmate calls. When a call is placed to a number that would be blocked for billing reasons, the called party is provided with the option for immediate access to our live Customer Care Call Center to establish billing arrangements. Typically, an account is established in 15 minutes, and inmate calling access is immediately allowed.  
- **Call Center Debit** – Call Center Debit allows inmates’ loved ones to fund an account associated with a specific inmate’s PIN. Once the account is funded, the money belongs to the inmate and is... |
- Integrated Cardless Debit – Integrated Cardless Debit is a fully integrated debit platform that allows inmates to place calls using the funds established and maintained in their individual PIN-based accounts. To enable this calling option, CenturyLink will interface with the facility’s inmate/records management system or commissary software package to share information between systems and automate the process. If an integration is not possible or if the DOC prefers, CenturyLink can also provide the DOC Facilities with physical debit cards sold through the commissary.

- Keefe-Integrated DirectLink Cardless Debit – When Keefe’s KeepTrak banking system is in place, we can offer our unique DirectLink Cardless Debit program. This service integrates the Enforcer with the Keefe KeepTrak banking system, enabling inmates to place calls using funds directly from their trust accounts. There is no need to open or fund a separate debit calling account; to transfer funds between two different accounts; or to manage a separate refund process for calling accounts.

**Funding Announcements**
The Enforcer can automatically notify inmates when funds have been added to their Debit calling account, or to a Prepaid calling account that is tied to a telephone number the inmate has called in the past. Announcements are automatically generated by the Enforcer system and delivered to a secure voice mailbox that can be accessed only by the designated inmate with the appropriate PIN.

**Inmate PINs with Optional Automatic Enrollment**
The Enforcer system accommodates the use of inmate personal identification numbers (PINs) for call tracking. Various numbering schemes are supported in order to best fit the existing inmate identification method in use at the facility. This ranges from adopting a number assigned by the facility booking system to assigning a new random unique number for calling to something in between. This will be customized based on the facility’s preference and with the goal of minimizing facility personnel time. Inmate accounts and PINs can be established automatically through a direct interface with the facility’s Offender Management System (OMS) or Booking system or through manual entry.

**Inmate PANs (personal allowed number lists) with Self-Learning Capability and Paper-Free Change Request Options**
The Enforcer system may be configured to require a list of Personal Allowed Numbers (PANs). This is a list of defined telephone numbers that each inmate is permitted to call. Each time the DOC activates the PAN feature for an inmate, you can select a maximum number of PANs to allow on an inmate’s list. If you leave the field blank the default value is 20, but there is no practical limit to the number of PANs that may be assigned.

**Self-Learning Mode:**
In order to minimize the time required to enter an allowed list for each inmate, the system provides a useful “self-learning” feature. Upon assignment of a PIN, the first telephone numbers to which calls are completed are added to the inmate’s PAN list, until the
<table>
<thead>
<tr>
<th><strong>Response to RFI</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automated Operator Service in Multiple Languages</strong></td>
</tr>
<tr>
<td>The proposed Enforcer provides fully automated collect, prepaid collect and optional debit calling. Access to live operators is neither required nor permitted at any time. The Enforcer is delivered with pre-recorded instructional voice prompts in both English and Spanish. Language is selected by the inmate as part of the call setup process. “For English, press 1; for Spanish, press 2.” Additional languages can be added at the facility’s request at no charge. Languages currently deployed at some of our client facilities include English, Spanish, French, Russian, and Hmong.</td>
</tr>
<tr>
<td><strong>Custom Call Prompts and Voice Overlays</strong></td>
</tr>
<tr>
<td>All call prompts can be customized at no cost to meet the DOC’s exact specifications. Also, the system is configurable to play random voice overlay announcements to notify the called party of the call’s origin. The announcement content is programmable along with the announcement volume and frequency.</td>
</tr>
<tr>
<td><strong>Inmate Name Recording</strong></td>
</tr>
<tr>
<td>When each inmate places the first phone call using their assigned ID/PIN, the system will ask the inmate to record his/her name. This recording will be stored within the Enforcer system and used for all subsequent phone calls made using that ID/PIN combination. This measure prevents inmates from “passing messages” and ensures that the called party is provided with the inmate’s name during the call greeting. If desired, inmate names may be recorded by the optional site administrator or by facility personnel at the time each inmate is booked. If there is an error during the recording or too much background noise at the time the name is recorded, facility personnel may reset the name recording function for that particular inmate using any Enforcer workstation.</td>
</tr>
<tr>
<td><strong>Inmate Voice Messaging</strong></td>
</tr>
<tr>
<td>Using the same messaging service developed for The Communicator℠, CenturyLink can provide inbound inmate voicemail. Revenue generated by this value-added service will be shared 50/50 with the DOC. CenturyLink proposes a $1.00 fee per message, of which the DOC would receive 50¢. Inmate Voice Messaging can also be used by authorized Jail staff to broadcast messages to one, many, or all inmates in a correctional facility. The Jail personnel simply types the message into the Enforcer, which then converts the message to synthesized speech and delivers it to the designated inmates’ voice mailboxes.</td>
</tr>
<tr>
<td><strong>Administrative Controls</strong></td>
</tr>
<tr>
<td>The Enforcer system provides centralized reporting capabilities, allowing facility users to generate reports immediately and in real time. The system comes preconfigured with an extensive list of standard reports. Additionally, a facility user can generate real-time “ad hoc” reports by defining his/her own query based on data of maximum number of PAN entries is made. To be added to the PAN list, a call to the telephone number must be accepted by the call recipient. Once the PAN list is full, any changes to the list must be made manually. Self-Learning can also be limited to a specified phone or phones in order to provide a greater level of control over the phone number entry process.</td>
</tr>
<tr>
<td>Feature</td>
</tr>
<tr>
<td>-------------------------------------</td>
</tr>
<tr>
<td><strong>Report Scheduler</strong></td>
</tr>
<tr>
<td><strong>Password Controlled Access</strong></td>
</tr>
<tr>
<td><strong>User Permissions – Editable Per User or Group</strong></td>
</tr>
<tr>
<td><strong>User Access Log</strong></td>
</tr>
<tr>
<td><strong>Court-Sealed Records</strong></td>
</tr>
</tbody>
</table>

**Fraud Controls**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Three-Way Call Detection</strong></td>
<td>The Enforcer automatically detects attempts by destination parties to connect, or forward, calls to a third party. These detection features have highly configurable parameters for changing the sensitivity to accommodate the requirements of each installation. When a three-way call attempt is detected, the system can either:</td>
</tr>
<tr>
<td></td>
<td>a.) flag the call for investigation;</td>
</tr>
</tbody>
</table>

interest – allowing instant access to any report you could ever need. Depending upon the user’s privileges, they are able to pull reports either for their specific facility or for all facilities in a network of jails.
| **Hook Switch and Secondary Dial Tone Prevention** | Inmates are not permitted to obtain secondary dial tone or to “chain dial” at any time. Any attempts to manipulate the inmate phone or hook switch in order to bypass system controls will result in immediate call disconnection, forcing the inmate to begin a new call with all call controls in full effect. |
| **Extra Dialed Digit Prevention** | The Enforcer monitors each call connection for any inmate attempts to bypass the system controls. If an inmate presses keys on the keypad following call connection, the system detects this activity and terminates the call. |
| **Chain Dialing Prevention** | The Enforcer counteracts fraud by preventing chain dialing, allowing completion of only one dialed number per individual attempt. Upon termination of each call, the inmate is returned to the call initiation script and required to go through the entire controlled process in order to place another call. |
| **No Incoming Calls** | No incoming calls are ever allowed with the Enforcer call processing system. The Enforcer system is hosted at the CenturyLink data center in San Antonio. All inmate calls are processed by this centralized system and terminated over outbound-dial only trunks. Additionally, the onsite IP Gateways that provide talk battery to the inmate telephones are incapable of processing an inbound call, and, as such, CenturyLink can warrant that no inmate telephone shall be capable of receiving an incoming call. |
| **Real-Time Call Validation** | CenturyLink’s call validation incorporates real-time validation responses from Local Exchange Carriers, compliance with carriers who do not permit collect calls, and managerial restrictions such as blocked-number lists. Call validation counteracts fraud by correctly identifying the location of called numbers to prevent the use of prepaid cell phones or pay phones to commit fraudulent activities. By validating numbers, we have the most up-to-date information about a BTN. |
| **Continuous System Monitoring** | As an additional fraud prevention tool, CenturyLink proactively monitors system data by looking for fluctuations in call traffic and failed attempts that could indicate fraud. |
| **Custom Call Restrictions** | Inmate calling can easily be limited to specific times of the day and set lengths of time. During installation, the system is programmed to block calls to live operators, toll-free lines, long-distance carriers, judges and correctional facility staff, etc. While these call restrictions are set facility-wide, additional call restrictions can be set for individual inmates. Inmates can also be restricted to calling only within a certain facility, or even within a designated area within a facility (such as in his or her housing area only). |

## Call Controls

| **Blocked Number Tables** | The Enforcer enables authorized users to immediately enter blocked numbers into the system using the user-friendly Administrator |
Blocks may be added for a specific telephone number or group of numbers. Important Block Features include:

- Block groups of numbers, such as: 800, 888, 866, 911, 1411, 555-1212, 1010XXX, etc
- Block individual numbers – unlimited quantity
- Blocks from your existing system will be imported during installation process
- Soft Block resulting from multiple refused calls
- Real-Time block activation
- Simple workstation block entry
- Blocked number report

Standard blocks are established for each system at the time of installation. These include directory assistance, 911, emergency, pay-per-call services, 1010XXX access codes, toll free numbers, and live operators. In addition, CenturyLink’s project team will work with the site to populate the blocked number table with facility personnel telephone numbers, and will work with the outgoing vendor to incorporate any telephone numbers which were blocked due to complaints of harassment.

<table>
<thead>
<tr>
<th>Configurable Call Duration and Velocity Limits</th>
<th>Call duration and velocity limits can easily be set by dialed number, individual inmate, inmate classification, inmate group, call type, pod, facility or system-wide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inmate Call Suspension and Automatic Reinstatement</td>
<td>The Enforcer supports the suspension of inmate calling privileges by PIN. Authorized personnel may enter a timeframe (i.e. 24 hours) or a specific date/time when the suspension is to end. At that point, the suspended inmate may only call legal counsel until the suspension period ends. When the suspension is over, calling privileges are automatically restored by the system. There are two categories of Suspension. Full means the inmate will not be allowed to place any calls, including calls to attorneys or free numbers. Standard is the default setting and allows the inmate to place calls only to attorneys or numbers that are identified as privileged numbers.</td>
</tr>
</tbody>
</table>
| Phone Shutdown | The Enforcer system is configured to support cut-off of the inmate phone system by individual phone or housing unit configurations in the event of a riot or lockdown, or any other incident that requires emergency shutdown of the inmate telephone system. **Electronic Phone Shutdown:** A single station, multiple stations or individual calls may be quickly switched on/off through the workstation Call Status display. All administrative changes made in the Enforcer system occur instantaneously in real time, so the time required for this action depends only upon the speed of the operator. Taking a station offline can easily be accomplished in less than one minute. Once the operator clicks Cutoff and Disable, the station is immediately taken offline and any call in progress is terminated. To allow calls in progress to complete, the operator can instead click Disable; this action will allow any call in progress to complete before disabling the
phone station from making further calls.

**Mechanical Phone Shutdown:**
Mechanical cut-off switches may be provided as an alternative to phone shut down using the system workstation. These manual overrides or “kill switches” are used to quickly turn the telephones on/off on demand. Multi-phone kill switches will be installed at each control center or as specified by the facility.

### Customized Call Branding

The Enforcer will be programmed with a customized call greeting played to the called party upon answer. Upon detecting answer, the system responds with "Hello, this is a collect call from [inmate name], an inmate at the (FACILITY NAME) Detention Center."

### Phone Scheduler

The Enforcer’s Phone Scheduler feature lets you pre-set any on/off times for the phones that you choose. The Enforcer can accommodate different schedules for days of the week, dates of the month and year, etc. Hours can be set as follows:

- By phone or group of phones (booking area, living units, infirmary, recreation, etc. may each have unique operating hours.)
- For all phones in the facility
- Unique hours for defined holidays
- Unique hours by day of week
- Unique hours for specified called numbers

### Positive Acceptance

The Enforcer system supports both DTMF and pulse-based call acceptance responses. When the called party is instructed to accept or reject the call, the system “listens” for either the appropriate DTMF or the correct count of rotary-dial pulses.

### Answer Detection

The Enforcer recognizes busy signal, ring no answer, and invalid number announcements (SIT Tones). Upon detecting answer, the system will only acknowledge positive acceptance by the called party. Answering machines, pagers and voice mail responses will all be treated as incomplete calls. Only a positively accepted call will generate a call charge to the paying party.

### Investigative Tools

#### 100% Monitoring and Recording of Non-Confidential Calls

**Real-Time Monitoring** -
Call monitoring is accessed through the Call Status tab of The Enforcer’s GUI. The authorized user selects a station or trunk to monitor with a click of the mouse, and then clicks the Connect button. This function is silent and undetectable by either the inmate or called party. Multiple monitoring sessions can occur at the same time without any impact to ongoing call processing or recording.

**Critical Call Monitoring Functions include:**
- Silent, undetectable monitoring
- Allows multiple simultaneous monitoring sessions
- Search function to isolate calls of interest
- Monitoring has no impact to recording function
- Ability to monitor from a remote workstation or PC via LAN,
WAN or Internet
- Protection of privileged calls from monitoring
- Ability to disconnect call in progress while monitoring
- Ability to “barge in” to calls in progress and speak to both parties

**Recording and Playback:**
The Enforcer system offers fully integrated digital recording capability with the option to record every call or to track only those phone numbers selected for recording. Call recordings are digitally stored online and will be available to the facility for immediate access throughout the contract duration.

Any individual desiring access to the recording playback or call monitoring must have a valid user name with sufficient privileges and a valid password. The Enforcer streams and copies recordings to system users through its monitoring and playback functions.

---

**Verifiable Security**

**Encryption on Call Recordings – Supported by Free Expert Testimony**

The Enforcer system utilizes its Pikamux call processing program to generate the call recording in a raw proprietary format. The system then utilizes its AU comp program to decode the Pikamux raw file and convert the recording into a Speex compressed format which supports playback utilizing various utilities. The AU comp program also creates an MD5 checksum of the Speex file. MD5 Sum is an open source program which will create an MD5 checksum of any file.

The process that has been implemented to confirm authenticity mandates that the MD5 checksum created by the AU comp program be recorded in a secure location. At the time of the authenticity test, the "expert" can use the MD5 Sum program on the recording and compare the resulting checksum to the checksum retrieved from the secure location. If the checksum comparisons are equal, this will confirm that the recording has not been tampered and is therefore authentic.

CenturyLink will also volunteer an expert to testify in any court proceedings regarding the security and verity of our call recordings.

---

**Crime Tip and PREA Lines**

The Enforcer system can be configured to support as many tip-lines and voice message lines as each facility requests. If an external tip line exists that the DOC prefers to retain, CenturyLink will simply program that number in for free calling and speed dial access (it can also be set as a privileged if the DOC would like only those staff members with access to the destination voicemails to be able to hear inmates leave messages). Otherwise, any and all message lines the DOC would like to create will simply be voicemail boxes on the Enforcer itself. Each will have a speed dial code clearly posted for the inmates and will be free (and privileged if the DOC so requests).

Each voicemail’s number (#123 for instance) can also have an alert set on it so that a designated facility investigator or administrator is notified immediately whenever an inmate dials the line. At the DOC’s discretion, each line can be set to allow access with or without PINs (to enable truly anonymous reporting as required by the PREA—
| **Officer Check-In (Optional)** | CenturyLink is proud to offer the DOC ICStracking™, our Officer Check-In service. While many inmate telephone service providers are now offering similar services, CenturyLink was actually the first in the industry to provide Officer Check-In services to our clients!

ICStracking™ was launched almost five years ago, in the summer of 2007. It offers the ability to capture and record corrections officers’ location via the inmate telephones using an ID/PIN assigned to the officer. Each officer will use a nearby inmate telephone to log in to the system and verify that they are working in that part of the facility. The check-in event is logged by the system as a call record and can be reviewed, reported, or generate an alert just like any other inmate phone call. There are no charges associated with this feature.

As an optional, added security feature, if your facility is utilizing The Verifier Voice Biometric feature the system will verify the officer’s voice against the voice print stored within the system associated with the Officer’s ID/PIN. This ensures that another officer or inmate is not attempting to check in on his/her behalf. |
| **Call Alerts (Hot numbers, hot PINs)** | The Enforcer provides an Alert feature to aid investigators in up-to-the-minute inmate telephone activity. The Enforcer alerts can be placed on specific Inmate PINs or specific destination numbers to indicate that the inmate or number is currently involved in a conversation. These alerts can be delivered in the following ways:

- Monitoring Alerts - The Enforcer can call an investigator on his or her telephone (or cell phone) and once provided with an approved pass code can immediately patch the investigator into the Enforcer monitoring session for almost instantaneous access to inmate activity. This capability is silent and undetectable by the inmate and the called party.
- Email/SMS Alerts – The Enforcer can send email or SMS message to an administrative workstation or any public email address when an alert is triggered.
- Paging Alerts - The Enforcer can issue numeric messages to paging services to alert an investigator. |
<p>| <strong>Funding Alerts</strong> | Our system allows investigators to set alerts on inmates of interest and/or telephone numbers of interest. When a Debit or Prepaid account is funded that is associated with an inmate or telephone number of interest, the designated investigators are immediately alerted via email. Email alerts contain information such as Inmate ID and Name (for a Debit account), names and addresses of account holder and account funder (for a Prepaid account), funding amount, and funding source (credit card, Western Union, cashier’s check, or money order). If a credit card was used, the alert will also report the first and last four digits of the credit card number. |
| <strong>“Find Me, Follow Me”</strong> | Find Me, Follow Me allows call alerts to phone multiple investigator telephone numbers (such as an office number, cell number, and home number), trying each number in succession until the investigator answers and enters the correct access code; this feature dramatically increases the probability than an investigator |</p>
<table>
<thead>
<tr>
<th><strong>Gang Management</strong></th>
<th>Reports on numbers dialed by multiple inmates or by multiple inmates out of a pre-defined group (such as all inmates identified in the OMS as members of a particular gang) is a standard part of the Enforcer’s Gang Affiliation tracking tools. The Enforcer can also provide a Gang Calling Analysis function, which shows additional members of the same gang and compares calling activity, and provides detail of multiple offenders calling the same number and their gang affiliations.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Remote Call Forwarding to Authorized Investigators with Ability to Barge In or Disconnect Call</strong></td>
<td>When a Hot Number or Hot PIN alert has been set, the Enforcer will call an investigator on his or her telephone (or cell phone) and once provided with an approved pass code can immediately patch the investigator into the Enforcer monitoring session for almost instantaneous access to inmate activity. This capability is silent and undetectable by the inmate and the called party. Once patched into the call, the investigator has the ability to silently monitor, barge into the call and speak to both parties, or disconnect the call.</td>
</tr>
<tr>
<td><strong>Searchable Call Notes</strong></td>
<td>Users may add notes or comments to a free-form field associated with each call record, Inmate Profile, or detail record for a called party number. This may include case numbers or investigator notes, or any information that the facility wants to record for future use. All notes are searchable by inmate ID, Called Number, User, Date &amp; Time, or by any text entered into the note. The Enforcer is configured to automatically add notes to a Number Detail Record when certain actions occur, such as a called party requesting a block on a phone number. These notes provide a history record of system-related events, call-related events, and user actions that occur on the number. These notes become a permanent part of the Number Detail Record, and appear at the bottom of the record.</td>
</tr>
<tr>
<td><strong>Unlimited Reverse Directory with Satellite Mapping</strong></td>
<td>CenturyLink provides our clients with Unlimited Reverse Lookup capability. This provides the facilities with integrated access to the desired reverse directory capability. From within a call record, the user can easily point, click and display the reverse directory info for the specified called number. The database is accessed via a secure link to the Internet and is constantly updated. CenturyLink will provide the subscription for the entire contract term and any extension terms at no charge to the DOC.</td>
</tr>
<tr>
<td><strong>Frequent Calling Reports</strong></td>
<td>The Enforcer comes programmed with a High Volume Users Report and a Frequently Called Numbers Report. The High Volume Users Report shows which inmates are placing an unusually high volume of calls. This may be indicative of fraudulent use. The Frequently Called Numbers Report shows which phone numbers have been receiving an unusually high volume of inmate calls, sometimes from multiple inmates. This can also be indicative of fraud or criminal activity occurring.</td>
</tr>
</tbody>
</table>
Kiosks/Tablets

Our proposed program consists of a portable media tablet, kiosks for downloading digital media and other content and a private delivery system.

The music catalog has millions of individual songs and is one of the largest music catalogs in the country. In addition to music, our media program can also support approved games, electronic messaging and photos as well as videos as proposed within this response.

The tablet can also work in conjunction with our Secure Mail Electronic Messaging program, allowing inmates to receive and respond to electronic messages directly from their tablet away from the kiosk. This exclusive feature maximizes the program’s efficiency by reducing the number of messages that need to be physically printed and distributed and provides a quick and efficient way for inmates to stay in contact with their loved ones.

In 2016, a 7" tablet will be introduced. Future enhancements of the tablet will include a number of new Self-Service inmate applications and share applications available on the inmate pod Kiosk. By enabling mobility of self-service applications through the Tablet, we minimize the need for inmates to congregate around inmate kiosks. The advanced Tablet will operate in offline mode until synced with our kiosk.

The Tablet will also include music, electronic messaging, games, movies, TV shows, facility content and educational content, videos and video visitation. It will also allow for inmate scheduling and facility/inmate communication/requests as well as the ability to order commissary and look up account balances.

Our proposed Digital Media Program is a proven, corrections-only program, currently operating in 16 DOC’s as well as the Federal Bureau of Prisons, servicing more than 525,000 inmates. Our technology partner, Keefe, has sold hundreds of thousands of players while delivering tens of millions of songs successfully inmates across the country. By far, Keefe has sold more players and songs in the corrections marketplace than any other provider.

Program Benefits:

Information Screen: Positive Owner Identification

- The Information Screen displays the offender name and number on the screen each time the device is powered on
- The Information Screen eliminates the need to etch or externally mark the property.
- This corrections-specific security feature reduces theft and allows correctional staff to easily manage the devices.
Reduced Property and Contraband
- The program significantly reduces property levels vs. other media programs.
- The program reduces the facility’s costs associated with ordering and managing radios, cassettes, or CDs.
- The device has no rotating motors or moving parts that can be used to make tattoo guns.

Media Library: Filtering and Control
- The media library can be filtered to remove any content that is explicit.
- The media catalog is updated with newly released content on a regular basis.

Easy for the Facility to Manage
- The program is designed to be self-service and requires virtually no interaction by facility personnel.

Life Skill Videos
Keefe has produced many Self-Help videos that would be available to the inmate. These videos can be easily viewed on the player and provide inmates with helpful information that will assist them upon their release. See the below list of Keefe produced Self-Help videos:

<table>
<thead>
<tr>
<th>Pre-Release Preparation</th>
<th>How to Rent Housing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective E-mails for your Job Search</td>
<td>How to Bag Groceries</td>
</tr>
<tr>
<td>Complete a Job Application</td>
<td>Time Management</td>
</tr>
<tr>
<td>A Positive First Impression</td>
<td>Reduce Stress</td>
</tr>
<tr>
<td>How to Tie a Tie</td>
<td>Relaxation: Niagara Falls</td>
</tr>
<tr>
<td>Job Interview Skills</td>
<td>Relaxation: Daytona Beach</td>
</tr>
<tr>
<td>Communication Skills in the Workplace</td>
<td>Relaxation: Boise Foothills</td>
</tr>
<tr>
<td>Managing Money Wisely</td>
<td>How to Wash Laundry</td>
</tr>
<tr>
<td>Creating a Budget</td>
<td>Meals on a Budget</td>
</tr>
<tr>
<td>Open a Bank Account</td>
<td>How to Inflate a Tire</td>
</tr>
<tr>
<td>Balance a Checkbook</td>
<td>How to Change a Flat Tire</td>
</tr>
<tr>
<td>Search the Internet Effectively</td>
<td>How to Perform an Oil Change</td>
</tr>
<tr>
<td>How to Open an E-Mail Account</td>
<td></td>
</tr>
</tbody>
</table>
Games
Keefe can provide games for the Digital Media Player. These games would be **FREE** to the inmate. The games available for **FREE** are *Ball Saver*, *Mighty Worm* and *Puzzle Challenge*.

MaxxPro4 MP4 Player
Keefe’s Media program features the *MaxxPro4* MP4 player which is available in an 8GB model. Additional *MaxxPro4* MP4 player specifications are detailed below:

- **3.5” LCD Screen**
  - The increased size of the TFT LCD color screen allows for easier viewing and navigation

- **FM Radio**
  - The player includes a built-in FM radio tuner

- **Clear Ear Buds**
  - High quality ear buds made of clear plastic and include a built-in antenna for maximum security. The antenna works in conjunction with the built-in FM tuner

- **Navigation**
  - Ability to easily navigate through the MP4 player menu options using the track pad which include scroll, select, volume, play and pause features

- **Clear Casing**
  - The *MaxxPro4* casing is made of clear plastic construction

- **AA Battery Powered**
  - MP4 player is powered by 4 AA batteries and can also be powered through an AC adaptor for longevity

- **FM Radio**
  - The player includes a built-in FM radio tuner

Menu Selections
The *MaxxPro4* also has the following menu options available (we can turn these features on or off as requested by the Department):

- FM Radio
- Mailbox
- Photo Album
- Video
- Games
- Catalog
7” Tablet
To be introduced in 2016, future enhancements of the Tablet will include a number of new self-service inmate applications. The tablet will also share applications that are available on thousands of our Inmate Housing Unit Kiosks located in correctional facilities nationwide. The advanced Tablet will operate in off-line mode until synced at our kiosks.

The Tablet will also include music, electronic messaging, games, movies, TV shows, facility content and educational content, videos and video visitation. It will also allow for include inmate scheduling and facility/inmate communication/requests as well as the ability to order commissary and look up account balances.

Tablet Features:

- Offering of different Tablet price points to reach maximum inmate ownership
- 7” Clear (front/back) tablet includes
  - DT M7 device with EMMC RAM
  - Signed firmware
  - Required certifications (FCC, UL, etc.)
  - MTK8127 Quad-Core 1.3 GHz
  - Android 5.0
  - 1GB DDR3
  - 8GB Storage
  - Micro-SD (Support up to 32GB)
  - 4-Directions gravity sensing
7” IPS Screen / 1024*600
• WIFI: IEEE802.11b/g/n wireless network
• Bluetooth 4.0
• HDMI
• GPS / Radio (FM)
• 5 Point Multi-touch Capacitive screen
• Front 0.3 Mp / Rear 2.0 Mp
• 3.7V/2800mAh
• Ear buds
• Manual
• On-board keyboard

Applications
• Media Player
• PDF Reader
• Clock
• Calculator
• Scheduling
• Media store
• FM Player
• Electronic Messages
• Electronic Photo Viewer
• Commissary ordering
• Trust Fund look-up

Content
• Music offering with all major labels
• Games –Free and for Purchase
• Books- Free Educational
• Videos- Free Life Skills and Educational videos, as well as videos for purchase

Education

Ability to allow both free and paid for content is recommended. Free content is readily available that focuses on GED prep and basic education to augment your agency’s education department. Khan Academy and Guttenberg books are both examples of free content. Paid for content is suggested through a Learning Management Systems (LMS) that allows a fully capability remote learning experience to achieve both a GED and post-secondary education. We recommend a vendor system that allows a customer input in conjunction with the vendor on the selection of LMS applications to run on the tablet.
Managed Access

Contractual Considerations

CenturyLink points out several important considerations if contraband cell phone technologies are to be bundled into the inmate telephone service contract.

First, each of the technologies presented have the potential for significant out-of-pocket costs. Perhaps more important, this area of technology – its deployment/operation and conformance with patent or other areas of law – is evolving. For any provider with the financial capacity and integrity to meet its commitments to fully assure/indemnify VADOC, this is a complex decision and it must be “priced in” to the financial offer. Some argue that controlling contraband cell phones drives inmates to the inmate telephone system and therefore “pays for itself”. While other providers may be able to show data to the contrary, in CenturyLink’s experience (2 full deployment sites) this does not occur.

Second, a separate contract for cell phone detection/control ensures that VADOC has complete control of the requirements and specific service delivered. It also ensures that it is not forced to pick, for example, an inferior inmate telephone system just because it came with a better cell phone control system.

Finally, tying this technology to the phone contract causes contract enforcement problems. For any contract, the main ways to impose sanctions for non-performance are (1) non-payment and (2) contract termination. By tying these two separate technologies into one contract, those methods are effectively taken out of the state’s hands. The only way to “not pay” the contract holder is to restrict its revenue stream (inmate communications) – but that can only be done at inmates’ and their families’ expense. And in order to terminate the contract for one system, it must also terminate and re-procure other services that may be performing satisfactorily. This can put the State in an untenable position with its vendor.

While CenturyLink is able to provide a MAS as part of any resulting contract, we do recommend an alternative approach. Specifically, we recommend requiring bidders to establish a Technology Fund through an up-front bonus and/or special per-minute charge, allowing VADOC to separately procure the technology. This approach is currently being used in different forms by the Michigan and South Carolina Departments of Correction.

Managed Access Product Description

Managed Access uses a DAS and attaches to it a group of cellular base stations that automatically control communications from contraband devices. Several companies provide Managed Access systems and CenturyLink is able to work with any of them. However, the response below is specific to the ShawnTech C5 System that CenturyLink has installed at the Texas Department of Criminal Justice, which was selected as part of a structured procurement managed by CenturyLink.
The ShawnTech solution, “Secure Communications/Mobile Device Interdiction”, is based on the ability to provide a few simple features:

- Detect the operation of an illicit cellular device within a defined secure wireless area
- Record relevant information for each illicit device, such as electronic serial numbers, make/model of phone, time/day of detection, and subscriber information
- Prevent illicit devices from communicating with the cellular network
- Provide easy-to-use tools for tracking activity, alarming tampering events, etc.

ShawnTech’s solution consists of six modes of operation:

- Network Analysis
- Intelligent Detection
- Location Identification
- Managed Access
- Redirection of Service
- Denial of Service

The System is designed to operate 24/7, and provides control of mobile devices within ShawnTech’s secure communication infrastructure, ensuring maximum capturing and controlling of unauthorized devices within the defined coverage area. The System will allow authorized devices (based on a device’s ID and SIM numbers) and all 911 calls to communicate and place calls.

In active mode, the System takes control of all powered on mobile devices within the defined secure area and verifies whether the device is authorized. For unauthorized devices, the System will proactively take control of the device and direct it to a Trojan control channel. The device will be held, it will not continue to scan the carrier network.

The System processes multiple formats simultaneously and detects any currently operating wireless service for voice, text, and data communications within the secure area, and is an independent System which does not interface with the commercial carrier’s network. It also does not require ongoing carrier support with the exception of Spectrum Agreements (which ShawnTech currently has completed).

A. Implementation, infrastructure and impact to inmate telephone system

The implementation plan for a facility-wide deployment of Managed Access typically takes about six months to up to one year, and includes installation of a DAS similar to that described previously, as well as on-site cellular control equipment. The total timeframe for installation is dependent on existing infrastructure (if use is allowed), the amount of inter-building connectivity required, and staff availability to oversee work in secure areas. Installation should have no impact on operation of the inmate telephone system.
The ShawnTech solution includes a secure multi-use infrastructure designed to the facility’s unique design and structure. The secure coverage areas (areas controlled by the solution’s wireless technology) are identified to maximize the capture and control of all unauthorized mobile devices within this coverage area.

The primary design is to focus on housing units and common areas used by the inmates, and then direct our design on selected coverage outside the buildings and structures. ShawnTech’s Network Operational Center (NOC) provides continuous monitoring and reporting of key equipment 24/7. This new infrastructure, like any DAS, can support both wired and wireless configurations for alternative uses, including inmate telephone, man down, land mobile radio (LMR) and other electronic communications services.

The System uses an all fiber backbone to connect the distributed antennas throughout the facility with the control units.

B. Oversight, auditing, and managerial processes

ShawnTech has developed several security measures and preventative maintenance procedures to ensure the System is secure and functional. These measures include monitoring at several layers so that authorized personnel and ShawnTech’s NOC technicians are notified of issues or compromised systems.

System monitoring logs include system shutdowns/power on, login access (failures and successes), IP address of remote system, and other data. The date and time of the incident, person reporting or resolving the incident, and final resolution notes must be recorded. Staff can enter notes and observations, and the logs can be accessed by VADOC staff at any time.

There are four emergency shut-off procedures for the System. All emergency shutdown procedures will be logged by the System with the ability to alert key personnel via text and/or e-mail messages. These alerts can occur periodically if desired (i.e. every 15, 30, 45, 60 minutes) until the System resumes normal operation. ShawnTech NOC technicians will also be alerted immediately and will initiate established monitoring procedures which may include calling a designated point of contact (POC) if desired.

The hardware elements of the System’s base station transceivers, as well as enclosures and power components, are packaged in tamper-resistant and tamper-evident cases.

The System is capable of scanning the active carrier networks in the area and comparing the results to previous results. Any change will be investigated, and any required change to communication channels will be implemented.
C. Process for updating hardware/software

The System utilizes a modular design, so system elements such as base stations can be added or replaced easily. The System is scalable and configurable, and the modular nature of the System reduces cost and complexity by simplifying the System configuration requirements.

The System is designed to ensure that future cell phone carrier technologies are easily accommodated, allowing the System to evolve and adapt through the addition or upgrade of new technologies in the form of replacement or additional base stations and other system elements. A Technology Refresh Warranty is included in the monthly warranty, maintenance, support and operational management service package.

Security features demonstrating that the device, network, and services are appropriate for use in a correctional setting, along with information detailing that the system contains appropriate IT security features.

CenturyLink Response: Read and understood.

Enforcer Inmate Telephone System Security Features

- **Hardened Corrections-Suitable Equipment**: CenturyLink has been providing correctional facilities with inmate telephone systems for more than 25 years. All onsite equipment is hardened and tested for use in correctional facilities.

- **Centralized Call Processing**: Call processing occurs on servers running in our secure data centers – leaving a much smaller footprint for equipment installed and maintained at your facilities. As a result, you will enjoy better performance, more space, cost savings, less onsite disruption, and higher facility security.

- **Verifiable Security Encryption on Call Recordings**: The Enforcer system utilizes its Pikamux call processing program to generate the call recording in a raw proprietary format. The system then utilizes its AU comp program to decode the Pikamux raw file and convert the recording into a Speex compressed format which supports playback utilizing various utilities. The AU comp program also creates an MD5 checksum of the Speex file. MD5 Sum is an open source program which will create a MD5 checksum of any file. The process that has been implemented to confirm authenticity mandates that the MD5 checksum created by the AU comp program be recorded in a secure location. At the time of the authenticity test, the "expert" can use the MD5 Sum program on the recording and compare the resulting checksum to the checksum retrieved from the secure location. If the checksum comparisons are equal, this will confirm that the recording has not been tampered and is therefore authentic. CenturyLink will also
volunteer an expert to testify in any court proceedings regarding the security and verity of our call recordings.

✓ **The Verifier Voice Biometric.** The Verifier matches an inmate’s ID/PIN and “voice print” created during the intake process with his/her voice when initiating a phone call. Summary follows:

- Provides option for self-learning, avoiding operational disruptions from enrolling the existing inmate population

- Provides detailed reporting capabilities on pass/fail rates, enrollment status, and other monitoring metrics. As an integrated feature within the Enforcer, call detail records are automatically updated with Verifier events for investigative review.

- Directly integrated into the Enforcer system, without the need to install or navigate to a separate “module”

- Provides a simple upgrade path to continuous voice biometrics

✓ **Fraud Protection Features List.** The Enforcer monitors all calls and prohibits inmate fraud at every step of the call process. The Enforcer provides an exhaustive list of features that detect and prevent fraudulent, illicit or unauthorized activity.

- **PINS:** Each time an inmate places a call, they are first required to enter their assigned PIN. By associating a PIN number with every call, the system provides investigators and security personnel with the ability to identify specific inmates when setting alerts, monitoring calls, retrieving call recordings, searching call detail records, generating reports, etc.

- **Custom Call Restrictions:** Inmate calling can easily be limited to specific times of the day and set lengths of time. During installation, the system is programmed to block calls to live operators, toll-free lines, long-distance carriers, judges and correctional facility staff, etc. While these call restrictions are set facility-wide, additional call restrictions can be set for individual inmates.

- **Random Voice Overlays:** The Enforcer system can play randomly interjected voice prompts as requested. These voice prompts can be custom recorded as requested by the facility, or a standard voice prompt such as this may be used: “This call is from a correctional facility, and is subject to monitoring and recording.” Voice overlays limit indicate where the call originated. Any inappropriate calls can be easily reported to facility personnel.
Real-Time Call Validation: CenturyLink’s call validation incorporates real-time validation responses from Local Exchange Carriers, compliance with carriers who do not permit collect calls, and managerial restrictions such as blocked-number lists. Call validation counteracts fraud by correctly identifying the location of called numbers to prevent the use of prepaid cell phones or pay phones to commit fraudulent activities. By validating numbers, we have the most up-to-date information about a BTN.

Continuous System Monitoring: As an additional fraud prevention tool, CenturyLink proactively monitors system data by looking for fluctuations in call traffic and failed attempts that could indicate fraud.

No Incoming Calls: All inmate calls are processed by this centralized system and terminated over outbound-dial only trunks. Additionally, the on-premise IP Gateways that provide talk battery to the inmate telephones are incapable of processing an inbound call, and, as such, CenturyLink can warrant that no inmate telephone shall be capable of receiving an incoming call.

No Chain Dialing or Hook-switch Flashing: Inmates are not permitted to obtain secondary dial tone or to “chain dial” at any time. Any attempts to manipulate the inmate phone or hook-switch in order to bypass system controls will result in immediate call disconnection, forcing the inmate to begin a new call with all call controls in full effect.

No Three-Way Calls: The Enforcer automatically detects attempts by destination parties to connect, or forward, calls to a third party. These detection features have highly configurable parameters for changing the sensitivity to accommodate the requirements of each installation. When a three-way call attempt is detected, the system can either

- flag the call for investigation;
- flag the call for investigation, and play a warning message to the inmate and called party; or
- flag the call for investigation, play a notification to the inmate and called party, and terminate the call.

The Enforcer monitors each call connection for any inmate attempts to bypass the system controls. If an inmate presses keys on the keypad following call connection, the system detects this activity and terminates the call. Any call terminated for this reason is marked accordingly in the call detail record.

Phone Shutdown. The Enforcer is configured to support cut-off of the system by individual phone, housing unit configurations, or facility in the event of a riot or lockdown,
or any other incident that requires emergency shutdown of the system, whether remotely or on-site by any user with the appropriate access level and login credentials. The system may be shut down at the demarcation location, by central control, and by select housing units. Phones may be shut down 24 hours a day, 7 days a week, including holidays.

**Kiosks/Tablets Security Features:**

- 7+ years of Proven Security software & systems for Tablet Hardware, Kiosks and Wireless Networks within a correctional environment is an important requirement for this technology offering.

- Device should only be able to connect to an approved vendor kiosk.

- Screen should display owner information including inmates name and number each time the device is powered on. The information screen will also indicate days remaining on the Mortality/Security Timer.

- “Mortality” is a key security feature. Mortality requires each device to connect to the Kiosk once every fourteen (14) days. The device will be disabled when the Mortality Timer reaches zero. The timer will be reset to fourteen (14) days each time the device is connected to the Kiosk.

- Expiration of the Mortality Timer should not affect any of the inmate’s content. The Department should have the ability to provide a different day range as determined by the Department.

- Any device that is stolen should have the ability to be fraud locked. Upon connection, a device that has been fraud locked should remain unusable until the facility reports the device as recovered.

- At each device sync, the media system must scan the handheld device for any contraband files and automatically remove any found contraband. Reporting of this activity should be provided to the DOC.

**B. The process that your company has for updating hardware and software.**

CenturyLink Response: Read and understood.

The Enforcer has unlimited expansion capabilities and will be able to accommodate any new construction or future growth of your facilities, at no cost the DOC. CenturyLink can add storage and phones at any time without affecting the operations of the existing system.
Free, regular software updates are provided throughout the life of the contract, always at no cost to the DOC. Whenever an upgrade and/or enhancements to the Enforcer system finishes testing and is ready for wide release, DOC personnel will be notified of the new release updates and provided documentation of the features and functions of the new software.

New software releases and enhancements are distributed through an IP connection, with no need for any onsite disruption. Enhancements and upgrades to the Enforcer are predominantly driven by market demand and specific client requests. Typically, large upgrades are released quarterly.

C. The ability of the proposed kiosk and/or tablet to allow commissary ordering. The Virginia DOC of Corrections currently contracts with Keefe for these services, and the contract expires in July 2017.

CenturyLink Response: Read and understood.

Our proposed Tablet solution will also include music, electronic messaging, games, movies, TV shows, facility content and educational content, videos and video visitation. It will also allow for inmate scheduling and facility/inmate communication/requests as well as the ability to order commissary and look up account balances.

As a particular benefit of our strategic partnership with Keefe, our proposed Enforcer inmate telephone system is able to enable commissary ordering by phone. Laminated menus are simply posted by the phones and inmates are able to post orders into an Interactive Voice Response system simply and easily…this frees up expensive kiosks to perform other higher-value tasks and/or provides a backup mechanism for commissary ordering.

D. The ability of the kiosk and/or tablet to download information (such as scheduling, medical, grades etc.) from the DOC’s Offender Management System.

CenturyLink Response: Read and understood.

Our proposed Tablet will also include music, electronic messaging, games, movies, TV shows, facility content and educational content, videos and video visitation. It will also allow for inmate scheduling and facility/inmate communication/requests as well as the ability to order commissary and look up account balances.

E. The ability of the kiosk and/or tablet to complete requests (such as grievances, scheduling etc.) from the kiosk and/or tablet.
CenturyLink Response: Read and understood.

Our proposed Tablet and Kiosk solution includes an inmate/staff communications module that allows for inmate scheduling and facility/inmate communication/requests as well as the ability to order commissary, look up account balances, and other services.

**F.** General pricing information regarding kiosks and related services along with the various different funding models offered by your company.

CenturyLink Response: Read and understood.

CenturyLink offers many services and options to go along with our program. Prices will vary depending on what services are added and what options are selected, along with the terms of the agreement and many variables such as the number of kiosks, wiring, integration, etc. In general, we recommend models where “cross-subsidization” across technologies is minimized.

**G.** Recommendations to the DOC regarding implementing an inmate electronic communications system that includes inmate telephone services, kiosks, and tablets.

CenturyLink Response: Read and understood.

As a general practice, CenturyLink recommends sourcing different technologies on different contracts. This is especially true for emerging technologies like Managed Access, but we also recommend sourcing inmate telephone services and kiosks/tablets on separate contracts. We firmly believe our inmate telephone and kiosk/tablet solutions are both “best of breed” and gladly offer them on a bundled basis; however, issues mentioned previously such as compliance with technical requirements across multiple platforms and contract compliance/enforcement issues are still potential problems.

General recommendations regarding inmate telephone services and kiosk/tablet solutions:

- Be careful of video visitation over wireless. The quality of wireless solution for video is still challenging. More important, mobile inmates with video access is a particular concern. We recommend video visitation only be able to occur on fixed kiosks.

- Offload as many tasks from kiosks to the telephone system (or to tablets) as possible. As the DOC is aware, kiosks are expensive to deploy and consume much more space than an inmate telephone or tablet. By offloading tasks to those systems, the overall cost to DOC constituents is minimized. In addition, transactions such as trust account balance inquiries or even commissary purchases are more secure over the phone system, since the user is able to be biometrically identified (through voice biometric...
verification) and the information is not visually presented to inmates potentially standing behind him/her.

- Check and score ALL references, not just the three hand-selected accounts typically provided in RFP responses. In addition, reference personnel should be no more than 2-3 layers of management from the top, and able to speak for the performance of the entire system (not just one site). Finally, we recommend asking references to compare the current provider’s performance against the prior provider. This is really the only way to get a comprehensive picture of providers’ commitment to service across each of its accounts.

- Pay particular attention to technologies underlying advanced services. For example, voice biometrics and keyword search are deployed very differently by different providers and should not be viewed simply as “check the box” items.

- Pay particular attention to customer service models for friends & family. With the increased scrutiny placed on these services due to ongoing FCC proceedings, this will become increasingly important over the next several years.

- Allow for multiple different financial offers in an initial round, but fix terms for a Best and Final Offer. For example, if commissions are to be provided, allow providers to offer different rate and commission offers in the initial submission, but fix rates and only allow for commission offers in a BAFO.

- Include specific transition services language in any resulting contract. Some providers rely on the fact that these services include critical security data that is housed on their servers. The DOC should specify that it owns the data, that any provider must continue to provide services for up to 6 months if a new provider is brought in, and that they must provide all DOC data to the incoming provider or the DOC at no cost to any party. Besides the obvious security benefits, this type of provision provides leverage to the DOC in case they must terminate the contract for non-performance.

H. Information about your company along with contact information of customers currently contracted with your company for both inmate telephones and kiosks and/tablets.

CenturyLink Response: Read and understood.

CenturyLink

Idaho Department of Corrections
Contact: Juliet McKay, Contract Officer
Phone: (208) 658-2176
Email: jmckay@idoc.idaho.gov

Nevada Department of Corrections
Response to RFI

Contact #1: Dawn Rosenberg, Chief of Purchasing and Contract Management
Phone: (775) 887-3219
Email: drosenberg@doc.nv.gov

Contact #2: Venus Fajota, Chief of Inmate Banking Services
Phone: (702) 486-9988
Email: vfajota@doc.nv.gov

Kansas Department of Corrections
Contact: Chris Walker, Communications Supervisor
Phone: (913) 727-3235 x 57101
Email: Chris.Walker@doc.ks.gov

Keefe

Wyoming Department of Corrections
Contact: Ron Thornton
Phone: 307-777-8971
Email: ron.thornton@wyo.gov

Nevada Department of Corrections
Contact: Dawn Rosenberg, Chief of Purchasing
Phone: 775-887-3219
Email: drosenberg@doc.nv.gov

Arkansas Department of Corrections
Contact: Mike Carraway, Assistant Director Admin Services
Phone: 870-850-8719
Email: mike.carraway@arkansas.gov

Note again that this is not a Request for Proposals, but rather a Request for Information (RFI) which gives vendors the opportunity to inform the DOC of the current capabilities available in the market. Information obtained may be used to develop requirements upon which a future procurement might be based.

CenturyLink Response: Read and understood.

4. DISCLOSURE OF SUBMISSION MATERIALS:
Vendors agree that by responding to this RFI they are granting a license to the VADOC for all data, materials and documentation originated and prepared for the VADOC pursuant to the RFI. Except for cost estimates, copyrighted or trademarked materials, such data, materials and documentation shall be subject to public inspection in accordance with the Virginia Freedom of Information Act. Proprietary materials that are submitted must be
identified by some distinct method such as highlighting or underlining and indicate only the specific words, figures, or paragraphs that constitute the cost estimates, copyrighted or trademarked materials in order for the VADOC to exempt them from disclosure.

CenturyLink Response: Read, understood and agree to comply.

Advice or assistance may be received from a vendor in identifying the features and characteristics needed by the agency; however, no person who, for compensation, prepares an Invitation to Bid or Request for Proposal for or on behalf of a public body shall (i) submit a bid or proposal for that procurement or any portion thereof or (ii) disclose to any bidder or offeror information concerning the procurement which is not available to the public. However, a public body may permit such person to submit a bid or proposal for that procurement or any portion thereof if the public body determines that the exclusion of such person would limit the number of potential qualified bidders or offerors in a manner contrary to the best interests of the public body (Code of Virginia, § 2.2-4373). The provisions of this act shall not affect the validity of any procurement contract entered into prior to July 1, 1997. This does not prohibit agencies and vendors from freely exchanging information concerning what is sought to be procured and what is offered.

CenturyLink Response: Read, understood and agree to comply.

5. QUESTIONS:
Any questions regarding this RFI should be directed only to:

Peter Batley, VCO, CPPB
Procurement Manager
Email: peter.batley@vadoc.virginia.gov
Phone: (804) 887-8233

CenturyLink Response: Read and understood.

6. RESPONSE DUE DATE:
Submissions are requested by 10:00 AM on March 28, 2016.

Please submit them electronically to:
peter.batley@vadoc.virginia.gov with subject line “DOC-16-079 re

CenturyLink Response: Read and understood.