



TEXAS DEPARTMENT OF CRIMINAL JUSTICE
REQUEST FOR OFFENDER TELEPHONE SYTEM
SOLICITATION NUMBER 696-IT-18-P014
VOLUME TWO

TABLE OF CONTENTS

VOLUME TWO, SECTION 1 - TECHNICAL REQUIREMENTS	2
VOLUME TWO, SECTION 2 - SOLICITATION COMPLIANCE AND EXCEPTIONS	213
ATTACHMENTS	251
ATTACHMENT F: PRELIMINARY IMPLEMENTATION PLAN	253
ATTACHMENT G QUALITY CONTROL PLAN	256
ATTACHMENT I: SAMPLE SCP REPORTS	274

VOLUME TWO, SECTION 1 – TECHNICAL REQUIREMENTS

L.8.2 Volume Two - Technical Portion of Proposal

Volume Two, Section 1 - Technical Requirements

- A. This section of the proposal shall consist of the Proposer's response to the requirements in Section C herein.
- B. Prospective Proposers shall ensure that all material submitted should be directly pertinent to the requirements of this RFP and shall be formatted as to the specific requirements of Section C.
- C. The Proposer shall also identify all exceptions it takes to the technical requirements in Section C of the RFP and all exceptions for which it requests approval.
- D. The Proposer shall cross-reference the specific section and page number of the Implementation Plan that details the policies and procedures relating to the specific section. This volume should include, but not limited to, the following items:

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

Per Amendment No. 4, Question and Answer 23, TDCJ clarified that only a project schedule with a timeline needs to be included in the proposal rather than a detailed Implementation Plan that is due within 30 days of contract award.

As a result of this clarification, the CenturyLink Team has followed TDCJ's direction to include a Project Schedule with timelines instead of an Implementation Plan. Therefore, we do not make specific cross-references to the specific section or page numbers of an Implementation Plan (because a detailed Implementation Plan was not required).

SECTION C - DESCRIPTION/SPECIFICATIONS/WORK STATEMENT

C.1 Background

The Department is responsible for the supervision of an estimated 148,000 incarcerated Offenders. The Department's mission is to provide public safety, promote positive change in Offender behavior, reintegrate Offenders into society, and assist victims of crime.

CENTURYLINK HAS READ AND UNDERSTANDS

C.2 Statement of Work

Pursuant to Texas Government Code, §495.027, the Texas Department of Criminal Justice, hereafter referred to as Department, requires a Contractor to install, operate and maintain an Offender Telephone System (OTS) for eligible Offenders confined in facilities operated by the Department throughout the State of Texas. Such OTS shall be provided by the Contractor without any cost to the State, in which the Contractor shall pay the Department a

commission of not less than forty percent (40%) of the Gross Revenue received from the use of the system, or any services provided.

The Contractor shall deliver a turnkey solution, compatible at all designated facilities, to include all necessary personnel, supervision, infrastructure, hardware, software, equipment, installation, operation, maintenance, support, materials, supplies, transportation and services (except as may be furnished by the Department as specifically identified within this Contract) and all things necessary for or incidental to, a fully functional, administered and managed Offender Telephone System without any cost to the State.

The Contractor shall be responsible for, at a minimum, the major requirements outlined. Specific deliverables associated with each major activity are identified where appropriate. A brief description of each major activity is included to ensure a common understanding of the services to be provided.

The specified requirements and standards will serve as the benchmark for monitoring the Contractor's performance.

CENTURYLINK HAS READ AND UNDERSTANDS

We have provided a comprehensive response that meets or exceeds all of the State's requirements as specified in Section C.2 and throughout the solicitation.

C.3 Scope of Work to be Performed

The Department will look solely to the Contractor for performance. The Contractor is responsible for all resources necessary to provide the services included in this Contract. Services shall be provided statewide, the locations of which are listed in Exhibit J.1, Site List. The terms, conditions and requirements of this Contract pertain to all Department locations unless otherwise stipulated. The Department reserves the right to add, delete or change site locations, and to increase/decrease the number of eligible Offenders and/or telephones per location or make other business decisions as necessary for the operation of the Department.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

1. **Proposer shall describe in detail, all features, functions and specifications of the OTS offered to the Department. Proposer is required to show, in detail, how the proposed OTS meets or exceeds requirements. (Section C.3.1)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

We comply with all requirements in the RFP including C.3.1.

The CenturyLink team is proud of our 9 year association with the Department. We believe our longtime partnership has proven we bring technology capabilities that set us apart from any other vendor. We have worked closely with the Department to deploy new and existing technologies to meet the needs of the State and its constituents.

We know this RFP is about the future and choosing a supplier that will meet your needs over the next several years. We believe our track record and our response to this RFP demonstrate that we will continue to bring value to the partnership going forward.

As outlined in Section C.3.1 – Functional and Technical Specifications/Requirements, we understand that the proposed OTS will provide prepaid and collect telephone service to eligible offenders. Below is a point by point response to the minimum requirements detailed in that section; followed by a detailed description of the proposed OTS.

- **Ensure that each eligible Offender or person acting on behalf of an eligible Offender may prepay for the service**

MEETS OR EXCEEDS REQUIREMENT

The OTS allows for customers on the allowed calling list to accept (1) post-paid collect calls, (2) prepaid collect, or (3) offender debit (also known as “offender telephone account”) calls. These first two calling options are billed to and paid by the called party while the third option gives the offender the ability to prepay for calls.

The Offender can add funds to their offender debit account to prepay for service from their commissary account. Through a secure integration, the OTS receives an electronic data feed on a daily basis from the Department with the transfer information. The e-imports application then updates the offender’s prepaid account.

The proposed OTS also allows any person acting on behalf of an eligible offender to prepay for offenders’ calls by either depositing money into an offender’s account or creating a prepaid account of their own.

Friends and family members can add funds to either an offender telephone account or their own pre-paid account via the following methods:

- Securus’ Correctional Billing Services (SCBS)
 - through the website: www.securustech.net
 - By calling our customer care center: Agents are available 24/7/365 to receive payments by phone, or
 - By mailing a check or money order to the SCBS P.O Box
- Jpay Outlet – Jpay provides friends and family a convenient website, mobile App, and call center they can use to add funds to accounts.
- Visiting one of more than 35,000 MoneyGram locations such as Walmart and CVS Pharmacy
- Visiting one of more than 58,000 Western Union locations.

➤ **Use a biometric identifier of the Offender making the call**

MEETS OR EXCEEDS REQUIREMENT



Advantage

The CenturyLink Team proposes the continued use of our biometric voice print solution for the Personal Biometric Identifier (PBI), which is resident in the OTS. Because each person's voice contains a unique detectable signature, voice print is a powerful method of authenticating an offender's identity over the telephone. We are able to continue the current biometric identifier without the need for costly and disruptive re-enrollment of the offender population.

Over our 9 year relationship we have enrolled 437,152 offenders successfully into the voice biometric system. There are currently 127,489 active users.

The PBI system was designed for noisy environments and has been deployed for over 23 years in local, County, State and International correctional institutions, including TDCJ for the past 9 years. Voice print works with traditional telephones, negating the need for expensive and potentially high maintenance alternatives utilizing specialized fingerprint readers or retina scan readers. Compared to other biometric techniques, the proposed PBI is simple to use, natural, nonintrusive and virtually maintenance free. Voice print is based on the realization that each person's voice contains a unique signature.

Using the process that we have developed with the Department staff over the last 9 years, each eligible Offender will be supervised, enrolled/re-enrolled and verified, in person, by the CenturyLink Team personnel. As described in more detail Section 3.1.1.D, this enrollment will include a dual verification process.

The system provides specific analytical reports for voice biometrics to provide detail on which sites have been enabled or disabled, which offenders are current enrolled in the voice biometric system, which offenders are enabled or disabled, which telephones are configured to be enabled or disabled, as well as groups of telephones and telephone numbers. The system also provides reports to show the failure and success percentages for each offender to indicate whether or not the enrollment should be reset for an offender who might have a high failure rate.

➤ **Oversee entry of Personal Identification Numbers (PIN's)**

MEETS OR EXCEEDS REQUIREMENT

Our OTS system has a highly configurable PIN function to meet the needs of correctional facilities. Since TDCJ offenders are already assigned PINs in our system, this eliminates the waste of time and resources that would be required of PIN entry into a new system. Not only would it save the Department man power and time, but current offenders will be able to continue using their account as normal, avoiding loss of calling privileges and complaints.

Data transfer of PIN information will continue to be achieved through the e-imports application's interface with the Department's OMS.

- **The Contractor shall provide and maintain a minimum of one (1) communication device per thirty (30) eligible Offenders at all facilities**

MEETS OR EXCEEDS REQUIREMENT

The CenturyLink Team will meet or exceed the Department's requirements. At a minimum we will maintain the 1 to 30 ratio. **Importantly, we have worked with the Department and incurred the additional expense to install phones at a ratio of 1 to 23 offenders today.**

Under the existing contract with the Department, we have has gone through additions, deletions and replacement of hardware. The CenturyLink Team has worked closely with the Department to seamlessly provide these changes with little to no interruption to services. We commit to the same "no interruption to services" approach when additions or placements are needed and we shall install and activate them within ten business days of written notification by the Department.

- **Generate reports to Department personnel on Offender calling patterns**

MEETS OR EXCEEDS REQUIREMENT

The OTS provides standard and customized offender calling pattern reports through our dedicated SCP report writer, Inter-Communication Evaluation and Reporting System (ICER), and THREADS. The OTS reporting system is completely configurable and virtually unlimited.

SCP Report Writer

The Secure Call Platform (SCP) has a dedicated report writer that provides investigative information based on the call detail records. Users can search and analyze call details on all calls placed from each offender telephone through SCP. These details include date, time, duration, telephone number, origination, destination, offender 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. Examples of reports TDCJ can generate are:

- Call Detail Report
- PAN Frequency Detail
- Offender Phone Report Balance
- Offender Phone Report Transactions

Inmate Inter-Communication Evaluation and Reporting System (ICER)



Exclusive

The Inmate Intercommunication Evaluation and Reporting System (ICER) detects completed calls made on the offender telephone system(s) between offenders, whether within an agency or between agencies across the country. The ICER system generates reports to investigators or authorized staff at the participating agencies of these events without transmitting any call audio.

For each offender-to-offender call, ICER identifies the offenders, their locations, the call date and times, and the outside telephone number or numbers they called to make the connection.

ICER is unique in the industry in that it detects conversations between offenders via an algorithm between offenders both within the Department and other correctional agencies, and provides report notifications to the Department. Because of this algorithm, ICER will detect inmate-to-

inmate conversations and is not dependent upon only reporting calls made by inmates to the same telephone number dialed during the same time period.

THREADS Reports

THREADS' powerful data analytics engine analyzes multiple types of facility data, such as offender communication records, public phone records, billing name and address, data from confiscated cell phones, financial data, and more to automatically generate focused leads for investigators. The following are examples of the most popular types of reports THREADS provides:

- **Statistical:** Includes all occurrences of a phone number or a bounce list of numbers in the database and the most frequently called numbers by an offender or person.
- **Linkage:** Generates graphical results that let you explore the relationships between your targets. This visual reporting tool is a quick way to understand who offenders are talking to and how the calls are related to other known numbers or offenders.
- **Working Group:** Working Group analysis uses a person's communication behavior and calling patterns to identify phone numbers and people of interest.
- **Correlation:** Identifies common contacts and phone numbers between offenders, persons, and workspaces. Through correlation reporting, investigators can identify common contacts between offenders as well as fraternization between offenders and facility staff.
- **Time-Based:** Provides reports based on the timing and frequency of an offender's or other person's communications.
- **Financial:** Identifies correlations between offenders and people based on the funding of an offender's account, including automatic upload of JPay financial data associated with trust and phone funding into the THREADS application.

- **Network all individual facility systems together to allow the same investigative monitoring from Department headquarters that is available at each facility**

MEETS OR EXCEEDS REQUIREMENT

CenturyLink's OTS provider, Securus Technologies, has invested millions of dollars and thousands of hours to develop a carrier-class centralized (network-based) system. Access to the OTS monitoring and recording systems are provided through a single portal located at <https://commandcenter.securustech.net> allowing authorized staff to monitor, playback recordings, and conduct other investigative functions from headquarters, each facility, or from other remote locations.

The network services are installed by Securus and provided at no cost the Department. The network-based system provides the Department and its many facilities with a centralized management solution. Each facility is connected to the centralized network-based system.

Secure access into the system is important for new and updated user profiles, and system configuration data are archived at the central site for secure management. Headquarters staff and facility users have the ability to login to the centralized site to monitor conversations or playback recordings and conduct other investigative functions. For all users, this simple-to-use portal provides authorized users anywhere, anytime access to a secure, encrypted, single point gateway to all applications and services provided by the OTS.

The OTS provides consistently reliable data protection and is the only point of entry for authorized users. System operators must have a security clearance based on passwords, user-IDs, and security levels to gain access to any individual feature of the OTS. Any configuration changes are tracked based upon user ID and managed through levels of security access. The capability exists to grant access to other authorized law enforcement agencies as directed and approved by the Department.

- **Provide on-site monitoring of calling patterns and customize technology to provide adequate system security**

MEETS OR EXCEEDS REQUIREMENT

The CenturyLink Team provided the Department with workstations at the facilities, as well as at headquarters and regional offices, as required by the Department. Access from workstations give the Department staff the ability to monitor offender calling patterns, as well as complete access to all security systems and administrative tasks. The ability to monitor offender calling patterns is not limited to a Department facility; the OTS supports remote secure password protected access to the OTS user interface. The user interface allows all authorized users to access these same security applications.

To access available call for live monitoring in SCP, an authorized user simply needs to log into the SCP user interface, click on the monitoring tab and the list of active calls available appears.



Live Monitoring through Guarded Exchange (GEX)

The CenturyLink Team also provides the Department monitoring through Guarded Exchange.

As calls are processed through the offender telephone system, and analyzed using Securus' Actionable Intelligence Potential (AIP™) scoring system. This data-mining software platform uses proprietary technologies that mine through phone calls, emails, financial transactions, and other information sources. This technology is used to identify and report variations in offender call patterns containing actionable intelligence information based on Six Sigma tools and statistical methods. The system utilizes a group of characteristics and attributes associated with offender behavior. Current and historical phone calls are statistically analyzed by algorithms measuring phone use, numbers dialed, frequency, ports, location, area codes, time of day, day of week and many other offender behavior patterns and characteristics. Patterns are then identified, stored, and "learned" by the system. Our Live Monitoring system analyzes call

The CenturyLink Team recently worked with the Department to offer Guarded Exchange call monitoring services, monitoring over 15,000 calls per month. This service has been used by both the Office of Inspector General (OIG) and the Criminal Investigative Division (CID) on numerous occasions to investigate suspicious activity, with GEX providing over 200 intelligence reports to the Department.

patterns and other information to generate a call queue packed with Actionable Intelligence Potential.

GEX investigators take the data produced the aforementioned proprietary software in order to review and analyze calls to uncover leads and deliver results to focus investigations and close more cases. GEX will also continue to take direction from the Department on all monitoring priorities.

➤ **Provide a fully automated system that does not require a Department operator**
MEETS OR EXCEEDS REQUIREMENT

The OTS is fully automated and never requires the assistance of a live operator. The OTS provides instructions and messaging to both the offender and called party during call set up to walk them through the process of placing and receiving a call.

The OTS provides the flexibility to configure (on/off) the ability for an offender to hear the call set up progression (ringing, answer, acceptance, admonishments played to the called party, etc.) or to mute the call set up progression until the call is accepted. Offenders and called parties cannot speak to each other prior to acceptance of the call. While the call is being set up, the appropriate automated messages will be played to the offender indicating the progress of the call, including why the call did not complete or that the call is being connected.

Only calls that are positively accepted by the called party will be connected and result in charges.

When the telephone is picked up, offenders will hear the following admonishment:

1. “For English press 1, For Spanish press 2” (in Spanish).
2. “For a Collect call press 1, for a Debit call press 2.”
3. “Enter your TDCJ ID number now.”

If the TDCJ ID number is invalid – the system will allow the offender 3 more attempts for a correct ID. If incorrect, the prompt will play “Please hang up and try again at a later time”.

For a collect call, after the TDCJ ID number is validated, the OTS will prompt the offender to do the following:

4. “Please dial the area code and number you wish to call.”
 - If the number is on the offender’s authorized calling list, the voice biometric process will then begin.
5. “At the tone, please state your name”.
 - Once the offender’s name is validated, the call progresses to the next level of voice biometric verification
6. The offender will then be asked to say “Texas Department of Criminal Justice”
 - If both voice biometric verifications are approved, the OTS will say “Thank you, I recognize your voice” and the call proceeds the call will proceed.

- If the verification is not approved, the offender will receive a message stating that the voice was not verified and the call will end, forcing the offender to start a new, fully-controlled call.
7. If the call is not “private”, the offender and called party will be notified that the call is subject to monitoring and recording. The called party must provide acceptance before the call is connected.

For an offender prepaid debit call, after the TDCJ ID number is validated, the OTS will prompt the offender to do the following:

8. The offender prepaid system will provide the offender with his/her account balance, followed by this prompt: “Please enter the area code and telephone number you are calling now. This will cost you (X) dollar and (X) cents for the first minute and (X) dollars and (X) cents for each additional minute, plus any applicable telecom and sales taxes.”
9. The voice biometric verification process described above in 5 and 6 will then take place.
10. Immediately following successful authentication of offender voice print, the OTS will say “Thank you, I recognize your voice” and the call proceeds
- If the call is not “private”, the offender will be prompted that the call is subject to monitoring and recording. The called party must provide acceptance before the call is connected.

The offender and the called party cannot speak to or hear each other during this time.

Prior to call acceptance the called party hears the following automated message:

- “Hello, you are receiving a collect / prepaid call from ‘John Doe’, an offender at the ‘facility name’. This call is subject to monitoring and recording.”
 - “To accept this call, press 1.”
 - “To refuse this call press 2.”
 - “To hear the rates and charges for this call press 7.” (Collect Calling Only)
 - “To block future calls to this number press 6.”
- **Ensure that no charge will be assessed for an uncompleted call and that the charge for local calls will not be greater than the highest rate for local calls for Offenders in county jails**

MEETS OR EXCEEDS REQUIREMENT

No charges will ever be assessed for uncompleted calls. The OTS is fully automated and requires that the called party positively accept each call. The called party will hear an admonishment announcing that the call is from an offender in a Texas Department of Criminal Justice facility. The called party will hear a menu of options, one of which requires them to accept the call. Only when the call has been positively accepted will the call be charged.

The proposed rate for local calls will adhere to the state statute and the Department requirement that the rate for local calls will not be greater than the highest rate for local calls for offenders in county jails.

➤ **Compile approved Offender call lists**

MEETS OR EXCEEDS REQUIREMENT



Advantage

One of the many benefits of continuing with the CenturyLink Team is that all of the Department's approved offender call lists are already in the OTS system. These call lists are the result of a rigorous verification process developed in concert with TDCJ over the past 9 years, and managed by CenturyLink staff. All verification data are stored for investigations purposes. This process is described in detail in our response to L.8.2 #39.

Once verified, the OTS e-imports application allows for the electronic transmission of those offenders' approved call lists, Personal Allowed Numbers (PANs). E-imports also supports the transmission of other offender-specific information such as the name and address of the person associated with each telephone number. These data will be beneficial for validating addresses of persons on offenders' visitor lists. A comprehensive explanation of e-imports can be found in requirement number seven.

Investigators can also correlate information for data mining when the Department uses the OTS for administrative and investigative purposes.

➤ **Verify numbers to be called by Offenders**

MEETS OR EXCEEDS REQUIREMENT

As stated above, CenturyLink will continue to provide our Enrollment Center to verify called party numbers – both up-front and ongoing – per Department requirements. Once a number is verified for a specific offender, that offender will have a predetermined set of personal allowed telephones numbers (PAN) to call, currently set at 20. When the offender places a call, the OTS will validate and verify that the dialed number is on the approved calling list of that offender. During this verification process, if the called number is to an Attorney, the OTS will not allow call monitoring or recording. The process for verifying called numbers and privileged numbers is described in detail in our response to L.8.2. #39 and #40.

➤ **Provide for periodic review by the state auditor of documents maintained by the Contractor regarding billing procedures and statements, rate structures, computed commissions, and service metering.**

MEETS OR EXCEEDS REQUIREMENT

CenturyLink is subject to Sarbanes-Oxley regulations and performs internal audits of TDCJ records. These include:

- Monthly CDR rate audits, which ensure the OTS charges the correct rates on every call per the contract.
- Results from our billing quality assurance team, who perform regular test calls to collect, prepaid collect and prepaid test accounts to ensure rating and billing accuracy.

These and any other records required by State auditors will be made available immediately upon request.

Overview of the Proposed OTS Platform

The Secure Call Platform (SCP) is a state-of-the-art, web-based system designed to provide TDCJ with the ultimate in offender call control and reporting. SCP's advanced features provide extremely powerful and flexible tools for controlling offender 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.

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, block/unblock offender telephone calls including those placed with ADA devices such as TDD, CapTel and secure VRS, and generate reports in real time.

SCP will support TDCJ 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 offender-calling information more quickly and reliably. The system is scalable and flexible, reducing labor demands by automating many tasks. Routine offender 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

SCP gives the Department control to customize the system to your specific needs, even as those needs change.

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 TDCJ
- 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 patented 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
- 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
- ICER- Offender – Offender identification
- Voice biometric verification with offender PINs
- 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:
 - Secondary dialing
 - Switch hook dialing
 - Black boxing
 - Hacking
- Velocity restrictions

Service Features

- 24x7x365 Network Operations Center monitoring
 - You operate around the clock, and so do we. 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 the dedicated TDCJ Technical Support Center we created just for the Department
- 24x7x365 end-user support through our in-house Correctional Billing Services
 - We are 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

TDCJ NOC monitoring, Technical Support, and End-User Customer Support all occur in Texas based centers.

CenturyLink and Securus combined employ over 2,300 Texans.

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

- 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
- Website funding
- Western Union funding
- MoneyGram funding
- Collect, prepaid collect (AdvanceConnect), and debit options
- Offender PINs
- Offender PANs
 - 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

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

Call Controls

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

Americans with Disabilities Act Compliance



The OTS includes all system equipment necessary to meet the requirements set forth by the Department. This includes all necessary hardware, software, telephone devices including Americans with Disabilities Act (ADA) compliant handsets, TDD devices, and terminals for VRS.

As the Department is aware, we have provided Video Relay Service (VRS) at two TDCJ facilities, and can work with the Department to expand this in the future.

Securus uses ZVRS/Purple for our VRS solution. Our VRS is a complete solution for correctional grade VRS services which incorporates FCC regulations as well as the offender call controls, management, and investigative abilities expected for offender calls.

Our VRS is fully integrated into our Secure Call Platform giving the Department more control and more benefits. The high level of integration between Securus VRS and SCP provides hearing impaired offenders with “equal access” to communication services while providing TDCJ the ability to provide, manage, and investigate offender VRS calls in a manner consistent with traditional offender calls. **VRS will be provided free of cost to TDCJ and there will be no additional costs to the called parties or the offenders.**



With Securus' VRS, the CenturyLink Team provides the Department with a VRS solution which does more than meet the requirements of ADA compliance.

VRS supports both types of VRS Calls:

1. Offender VRS Phone to VRS Phone:
2. Offender VRS Phone to Standard Non-Video Phone:

Offender VRS call to F&F VRS Device

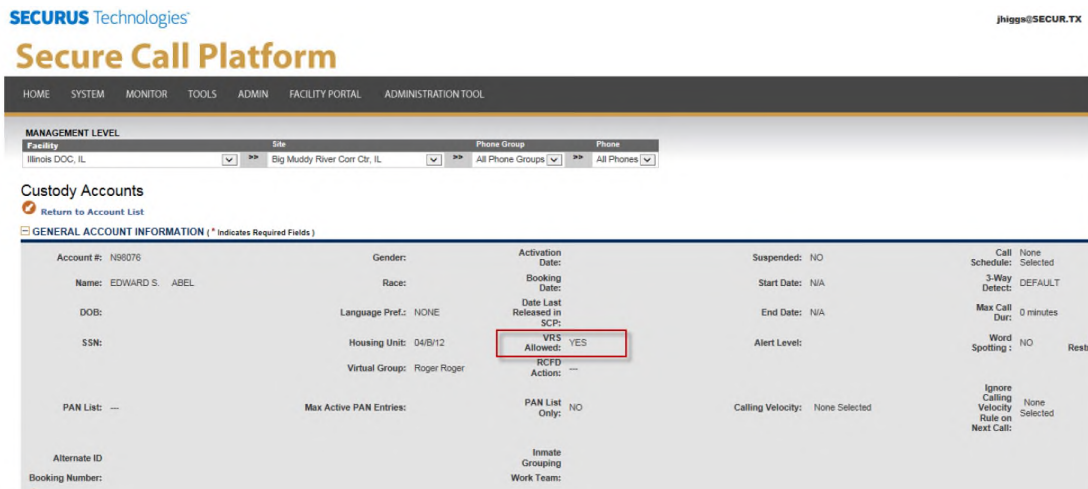


Offender VRS Call to Non VRS Phone Number



Controlling Which Offender May place VRS Calls

Authorized TDCJ users can set whether an offender is eligible to use VRS from the offender custody account profile page. For the Department we will configure the VRS application to require offender login. Then, the offender must have the “VRS Allowed” setting on the offender profile set to “yes” before they are allowed to login to the application.



The Securus VRS application will require offenders to enter both their designated offender ID as well as their issued calling PIN before being allowed to place VRS calls.

Call Controls

Standard SCP policies, such as PAN list control, call recording, time limits, redial prevention, and more are all functional on VRS calls because the system is fully integrated within the SCP. VRS highly leverages the standard offender call management control structures used by SCP for traditional offender calls, including the following:

- Calling Schedules
- Max Call Duration controls
- Calling Restrictions
- Calling Velocity
- Specific called party phone number controls both globally and on offender PAN lists
- Control over which calls to record


TDCJ benefits from the industry's only integrated Video Relay System (VRS) designed for the hearing impaired. VRS calls, like all other OTS calls, are stored and searchable in SCP. Our dedicated TDCJ Account Team has developed a special registration process for the hearing impaired within the CenturyLink Enrollment Office along with training videos, collateral material and call acceptance admonishments that are unique to TDCJ.

VRS Call Recordings

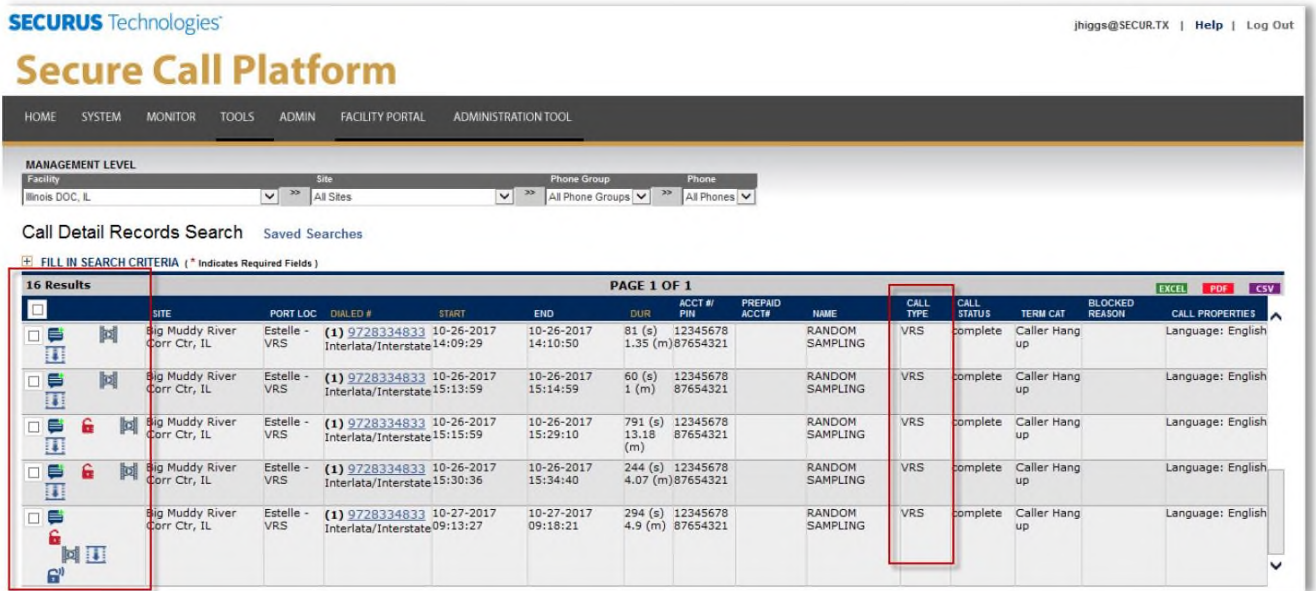
The nature of our relationship with Purple along with the proprietary integration of technologies, allows SCP to record VRS calls while still remaining compliant with FCC regulations. Because of the full integration of VRS with SCP, call recordings are searchable within the platform and will appear in the Call Detail Record.

VRS call recordings include the visual component of the offender call for both the offender and the other end of the video portion of the VRS call. Recorded VRS calls are available for download in MP4 format and can be put on a CD for investigative purposes.

VRS Call Detail Records

Like all other calls placed through SCP, a CDR is created for every VRS call. Authorized users can search VRS call records in the same way they search for any other records in the SCP portal. From the CDR, users can playback VRS recording by clicking on  icon.

Example of VRS CDRs:



SECURUS Technologies | jhiggs@SECUR.TX | Help | Log Out

Secure Call Platform

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL ADMINISTRATION TOOL

MANAGEMENT LEVEL
 Facility: Illinois DOC, IL | Site: All Sites | Phone Group: All Phone Groups | Phone: All Phones

Call Detail Records Search Saved Searches

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

16 Results PAGE 1 OF 1

SEARCH	SITE	PORT LOC	DIALED #	START	END	DUR	ACCT #/ PIN	PREPAID ACCT#	NAME	CALL TYPE	CALL STATUS	TERM CAT	BLOCKED REASON	CALL PROPERTIES
	Big Muddy River Corr Ctr, IL	Estelle - VRS	(1) 9728334833 Interlata/Interstate	10-26-2017 14:09:29	10-26-2017 14:10:50	81 (s) 1.35 (m)	12345678 87654321		RANDOM SAMPLING	VRS	complete	Caller Hang up		Language: English
	Big Muddy River Corr Ctr, IL	Estelle - VRS	(1) 9728334833 Interlata/Interstate	10-26-2017 15:13:59	10-26-2017 15:14:59	60 (s) 1 (m)	12345678 87654321		RANDOM SAMPLING	VRS	complete	Caller Hang up		Language: English
	Big Muddy River Corr Ctr, IL	Estelle - VRS	(1) 9728334833 Interlata/Interstate	10-26-2017 15:15:59	10-26-2017 15:29:10	791 (s) 13.18 (m)	12345678 87654321		RANDOM SAMPLING	VRS	complete	Caller Hang up		Language: English
	Big Muddy River Corr Ctr, IL	Estelle - VRS	(1) 9728334833 Interlata/Interstate	10-26-2017 15:30:36	10-26-2017 15:34:40	244 (s) 4.07 (m)	12345678 87654321		RANDOM SAMPLING	VRS	complete	Caller Hang up		Language: English
	Big Muddy River Corr Ctr, IL	Estelle - VRS	(1) 9728334833 Interlata/Interstate	10-27-2017 09:13:27	10-27-2017 09:18:21	294 (s) 4.9 (m)	12345678 87654321		RANDOM SAMPLING	VRS	complete	Caller Hang up		Language: English

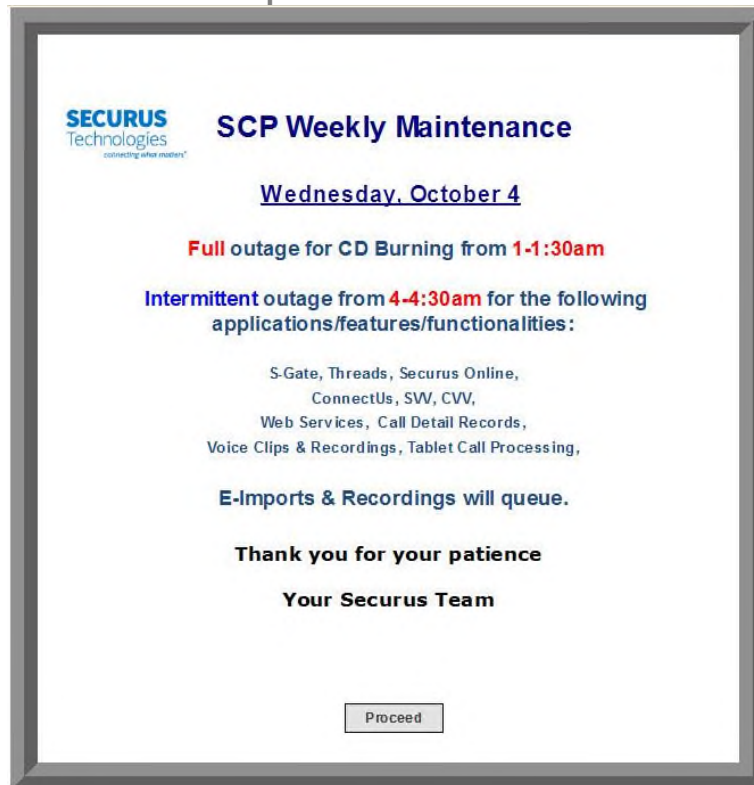
Software Upgrades at No Cost

The CenturyLink Team provides upgrades to the OTS system three to four times annually through a proven and tested after hours process that allows all sites to immediately realize the benefits of each upgrade. Our system delivers proven features driven by input from the most recognized corrections and law enforcement agencies in the nation.

Upgrades or version releases of SCP will only be made after the Department is advised of changes. Notification to the Department of upgrades will come from the dedicated TDCJ Account Manager, Paula Parson. In addition, maintenance events are always preceded by a splash screen displayed at the SCP portal 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. With all upgrades we provide release notes and instructor led training so that TDCJ personnel is always up to date.

The following image shows the sample splash screen that notifies users of upcoming maintenance.

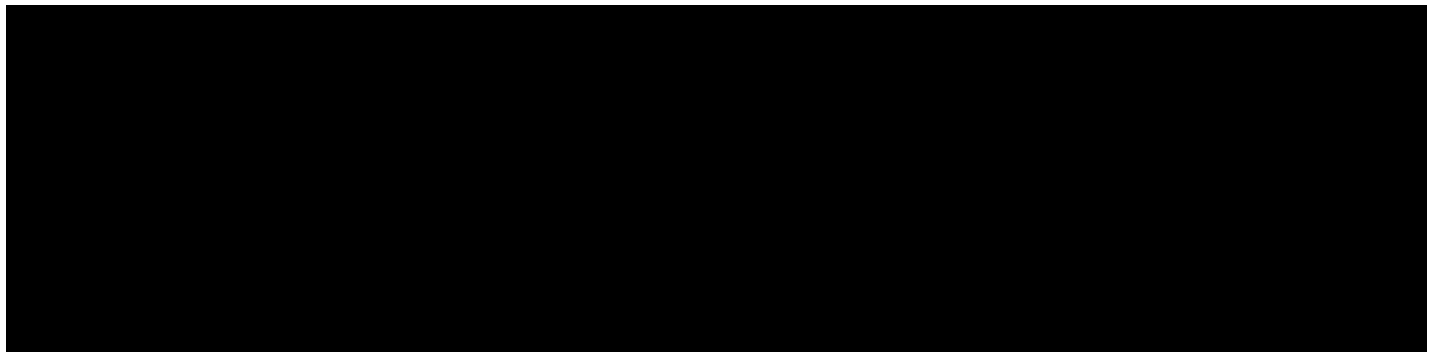
Splash Screen

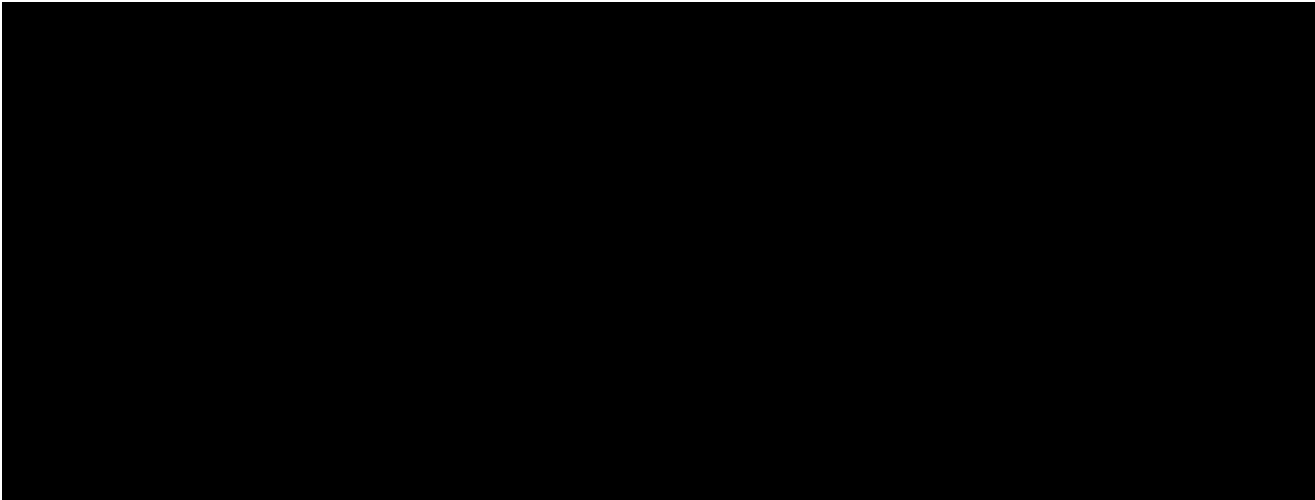
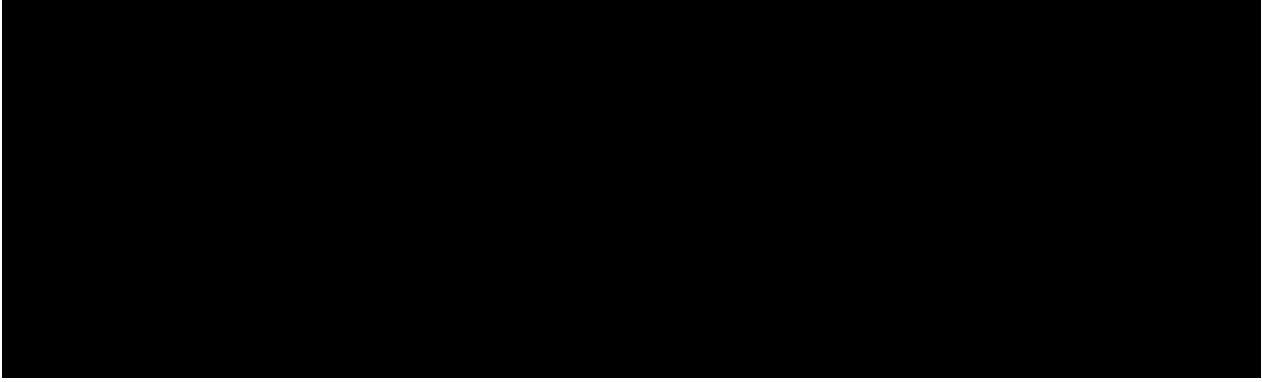


2. **Proposer shall describe in detail and provide specifics on how the attorney client communications will be protected to include the accuracy and updating of information from any State Bar Association. Proposer shall also provide detail on how attorney-client communication will be protected should an Offender's attorney reside outside of the State of Texas (Section C.3.1.1.C)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

Similar to Called Party registrations, attorney numbers are subjected to rigorous verification. The importance of this process is obvious, given its potential impact on attorney-client privilege.





Attorney Audit Process

The Enrollment Center also conducts quarterly audits of all attorney numbers. This is completed through a LIDB query that is verified against the OTS and Texas (and out of state) bar associations to flag and investigate any discrepancies. As part of the process, we verify that all cell phones were registered as cell phones and not later ported from a landline to a cell phone. We verify that the telephone number listed on the state bar website is the same telephone number the attorney registered originally.

Attorney Calls Marked as Private

The OTS has a standard feature that allows for attorney client privileged calls to be marked as private. Once this “Private” feature is enabled, this ensures on a global OTS basis that attorney client calls will not be monitored or recorded.

The “Private” feature also allows the Department to authorize and designate any other telephone number(s) as private. The administration of this feature is accessed through the SCP portal by authorized users.

3. **Proposer shall describe in detail the blocking function. Proposer may propose other similar numbers that should be blocked. (Section C.3.1.1.C)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The OTS provides blocking functions for both authorized Department Staff and Friends and family.

Blocking by Authorized Department Staff

The Secure Call Platform (SCP) allows authorized facility personnel to manage blocked numbers using the SCP user interface. Blocked numbers can be applied at various levels—facility, site, phone group, phone and offender. SCP offers unlimited blocking so the resulting call blocking table that is created may contain as many entries as needed.

The following are examples of how the Department can use the OTS blocking function:

- **Global Blocks** – These are numbers that are prohibited to all offenders in the TDCJ system.
- **Facility initiated blocks** – Facilities can create a block list for numbers that apply just to the offenders located in their facility. They can also block numbers being called by a single specific offender or from a specific phone.
- **Crime Victims** – The ability to call telephone numbers for crime victims can be blocked.



Advantage

We have already established an extensive list of blocked numbers with the Department and its facilities, saving the Department the time and effort creating those lists from scratch with a new provider.

From using our OTS system for the past nine years, the Department is aware that the system is completely programmable to block offenders from calling any telephone number, including but not limited to the following: local direct, credit card, third number, 1+, sent paid, all 0, 700, 800, 888 (includes all toll free area codes) 900, 976, 950, 911, and 10xxx. Additionally, there is an associated “Note” field that allows for additional information to be attached to a blocked number.

CenturyLink will receive and process any other written orders from the Department to block telephone numbers.

Blocking by Friends and Family

The OTS’ automated operator also provides a Perma-Block process for friends and family, which allows them to block the offender from calling their number permanently. The ability to immediately block calls helps reduce the number of called party complaints.

During the call process, the automated operator will provide the called party with the option “To block future calls to your number press 6.” The called party then presses the indicated key. The system will confirm with the called party that they would like their number block. Upon confirmation, the system will automatically block future calls.

If at any time, someone wants to unblock their telephone number from receiving calls from a TDCJ offender they can call our customer care agents and they will assist in processing the request.

4. **Proposer shall describe in detail, how the outward calling mode will prevent connections to pre-paid cell phones and virtual number telephone services. (Section C.3.1.1.C)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The OTS takes several steps to prevent calls to pre-paid cell phones.

Up-front Verification

Connections to pre-paid cell phones and virtual number telephone services occur on the front end of the process. Through the enrollment process established by TDCJ and managed by CenturyLink, non-eligible services – specifically pre-paid cell phones and virtual number services – are not allowed to enroll.

Virtual number services are simple to identify through a Line Information Database (LIDB). Over the years TDCJ and CenturyLink have worked collaboratively to establish and implement a comprehensive list of virtual number Operating Carrier. By querying LIDB, CenturyLink can extract the Operating Carrier Number (OCN) and flag virtual number services up-front, informing the registering party of TDCJ’s policies.

The CenturyLink Team will continue to offer our current TDCJ-dedicated Enrollment Center personnel, without needing to establish new systems, infrastructure, and processes for TDCJ.

The process to identify post-paid vs. pre-paid cell phones is more complex. LIDB does not separate pre-paid vs. post-paid services (e.g. Virgin Mobile and Sprint Post-Paid are the same OCN). As a result, per Department directive CenturyLink performs a three-way call with the cell phone carrier to determine the consumer’s billing status. A flowchart of the online and offline verification processes for cell phones is provided in our response to L.8.2. #39 below. Because these flowcharts are proprietary, we refer reviewers to these sections to avoid excessive redactions.

Fraud Management

CenturyLink carefully manages fraudulent attempts to enroll, which are significant in number. Suspicious/fraudulent attempts are flagged within our system, and follow-up attempts require manual intervention, including review of signatures among different forms, and other checks.

Ongoing Audits

CenturyLink receives daily booked, release, and update files from TDCJ to maintain an active offenders list and to update customer account status. We also receive a monthly active offenders list as a method to audit these daily updates, and perform other periodic audits for TDCJ. These include monthly audits of 10% of F&F accounts (all eligible PANs audited at least once annually). Cell phone customers who have changed carriers are automatically deactivated and required to re-enroll.

5. **Proposer shall describe in detail, how remote access to the system is accomplished as well as security features to prevent unauthorized access. (Section C.3.1.1.C)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

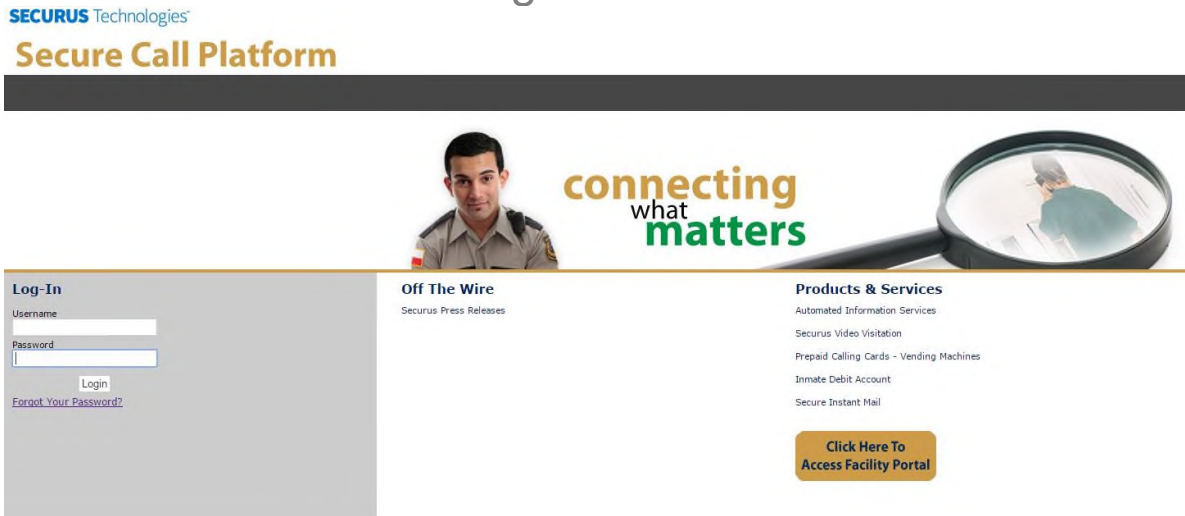
SCP’s user interface is the Department’s window to all of its features. Because it is entirely web-based, authorized users can access the system at any time, from any location through the same process. This design delivers investigative recordings with digital clarity and provides easy remote monitoring from any secure web browser with Internet access.

This system is built to allow our customers complete control over their systems in a simple, reliable, secure environment. Authorized users can easily apply settings and configurations to turn on a phone, restrict a phone, change a blocked number, and turn on or off features and applications — all in real time.

Remote access to the SCP user interface is accomplished in the following manner:

1. Authorized user opens Internet Explorer and enters the URL: <https://commandcenter.securustech.net>
2. The user will see the screen below
3. The user will be prompted for a user name and password
 - a. First time users will be given a temporary generated password. Once they enter the SCP portal they will be required to change the password.
4. Once the user name and password are validated the full suite of applications approved for the user are available.

Login Screen



Security Features

Each user has access rights assigned by the administrator, allowing the Department to control access based on the facility’s security clearance objectives. Administrators can limit individual access to each application, and can also limit access to each function within each application. A

user log documents the user, time of access, and accessed modules as an added security measure.

For even more security and control, user access can be programmed to restrict users to specific IP addresses within certain time limits. For example, a user could be restricted to access the SCP user interface from their workstation (and only their workstation) between the hours of 8:00 AM and 5:00 PM and their access blocked outside the facility.

Securus applies a high level of security to protect against cyber-attacks. Applications transmitting data across public networks support SSL, Certs, and encryption. This connection is established prior to the movement of any data across the network that is confidential or related in any way to the recordings, CDR data, etc. This complex encryption method prevents access or the potential intercept of this data and allows the communication access across the public network to be safe and secure.

Cisco and Juniper firewalls, used throughout the network to protect SCP and our customers, create DMZ networks. All servers, laptops, and workstations require anti-virus and anti-spyware protection software and the latest operating system patches. Securus supports both AVG and Symantec anti-virus.

The SCP portal has a multi-level password scheme that requires the following password standards to be utilized:

- The user ID jsmith@tdotx.tx is used to determine that the individual is authorized to only access applications determined to meet the appropriate clearance level
- For security purposes the system can also be configured to require a user password be updated/changed every 30/60/90 days or as required by the Department
- The user ID can be constructed using the user's first initial and last name or any combination authorized by the facility to create a unique user ID
- The user's password must be 4 – 14 characters in length, with at least one upper case letter and one numeric character, and must not contain spaces or blanks. Special characters are permitted
- The system can also be configured not to allow users to reuse previously used passwords

The current SCP password requirements in use today at TDCJ facilities are below. If at any time the Department would like to edit these standards, our team will assist in that process:

- Minimum Password Length – 8
- Maximum Password Length – 14
- Expires every 30 days
- Cannot use the last 12 passwords

Audit Logs

The SCP audit and tracking feature logs each user's specific activities for investigative purposes. As an example, when a user accesses a recording, SCP will mark whether the recording was played back, live monitored, copied to a management folder, downloaded or burned to a CD. This information is accessible by authorized department staff through SCP in a

user friendly report. This report provides the capability to search by individual user or by specific event, such as all recordings accessed for playback.

Additionally, the audit and tracking feature logs:

- When a user logs in to the system
- How long a user stays in the system
- Which recordings were monitored or played by a specific user
- What the user did with a recording
- Changes to custody accounts
- Changes to Personal Allowed Number (PAN) lists
- Changes to Global List entries
- Changes to security templates

Sample Recording Audit Log Search

SECURUS Technologies™
dinar@SECUR.TX | Help | Log Out

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL ADMINISTRATION TOOL REVERSE BNA LOOKUP

MANAGEMENT LEVEL

Facility: Securus Demo Site | Site: All Sites

Recording Audit Log Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches)

Username:

First Name:

Last Name:

Recording Usage: -- ALL --

Dialed Number:

Account #:

PIN #:

Call Start:

End:

Expiration Start:


End:

Access Start:

End:

2 Results PAGE 1 OF 1

ACCESS TIME	RECORDING USAGE	NAME	ACCT # PIN	CALL START TIME	CALL END TIME	EXPIRATION DATE	USER	DIALED NUMBER
04-12-2018 10:02:04	PLAYBACK	SOPHIE SUN	170701 170701	04-03-2018 11:56:12	04-03-2018 11:56:20	05/03/2018	dinar@SECUR.TX	2143945748
04-12-2018 10:00:36	PLAYBACK	SOPHIE SUN	170701 170701	04-03-2018 11:56:12	04-03-2018 11:56:20	05/03/2018	dinar@SECUR.TX	2143945748



Terms and Conditions
© 2005, 2011, 2015 Securus Technologies, Inc. All Rights Reserved.

This tracking mechanism is also integrated throughout the call detail reports in order to give authorized department staff a quick view to determine if a call had been accessed while running a standard call detail report. This indication of the recording accessed will show up in the form of a “padlock” icon. Authorized staff can click on the “padlock” and view the complete call access history details including Access Date, Access Type, User, Dialed Number, and Access Protocol if the session was via Department facility or remote access.

MANAGEMENT LEVEL

Facility	Site	Phone Group	Phone
Securus Demo Site	All Sites	All Phone Groups	All Phones

Call Detail Records Search

Saved Searches

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

29 Results PAGE 1 OF 1 EXCEL PDF CSV

	SITE	PORT LOC	DIALED #	GEO LOC	START	END	DUR	ACCT #/ PIN	PREPAID ACCT#	NAME	AGENCY TYPE	CALL TYPE	CALL STATUS	TERM CAT	BLOCKED REASON	CALL PROPERTIES
	Securus Demo Site	LP 1	(1) 9722770648 Local		02-13-2018 11:56:11	02-13-2018 11:56:40	29 (s) 0.48 (m)	77547 777547		CHRISTOPHER DOLITTLE		Debit	complete	Called party hangup		Language: English Voice Biometrics JPro Pin Check CVV Charge: \$3 Taxes & Fees: \$0.32
	Securus Demo Site	LP 1	(1) 9722770648 Local		02-13-2018 12:05:03	02-13-2018 12:05:37	34 (s) 0.57 (m)	77547 777547		CHRISTOPHER DOLITTLE		Debit	complete	Called party hangup		Language: English Voice Biometrics JPro Pin Check CVV Charge: \$3 Taxes & Fees: \$0.32
	Securus Demo Site	LP 16	(1) 9722770379 Local		02-13-2018 12:06:48	02-13-2018 12:07:11	23 (s) 0.38 (m)	6311 6311		KEN BURNS	FLDOC	Debit	complete	Called party hangup		Language: English Voice Biometrics Charge: \$3 Taxes & Fees: \$0.32
	Securus Demo Site	LP 1	(1) 9722770648 Local		02-13-2018 12:50:12	02-13-2018 12:50:31	19 (s) 0.32 (m)	77547 777547		CHRISTOPHER DOLITTLE		Debit	complete	Called party hangup		Language: English Voice Biometrics JPro Pin Check CVV Charge: \$3

Save selected calls to folder

6. Proposer shall describe in detail, how onsite and remote shutdown of the system is accomplished as well as security features to prevent unauthorized shutdown. (Section C.3.1.1.C)

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The OTS has the capability for the immediate shutdown of a single telephone, single facility, group of facilities, or the entire OTS. Shutdowns can occur through the SCP portal either on-site or remotely in accordance with predetermined access rules.

SCP provides multiple ways for an authorized user to shut down the system quickly and selectively which include:

- On/Off Station Control
- Programmable Calling Schedules

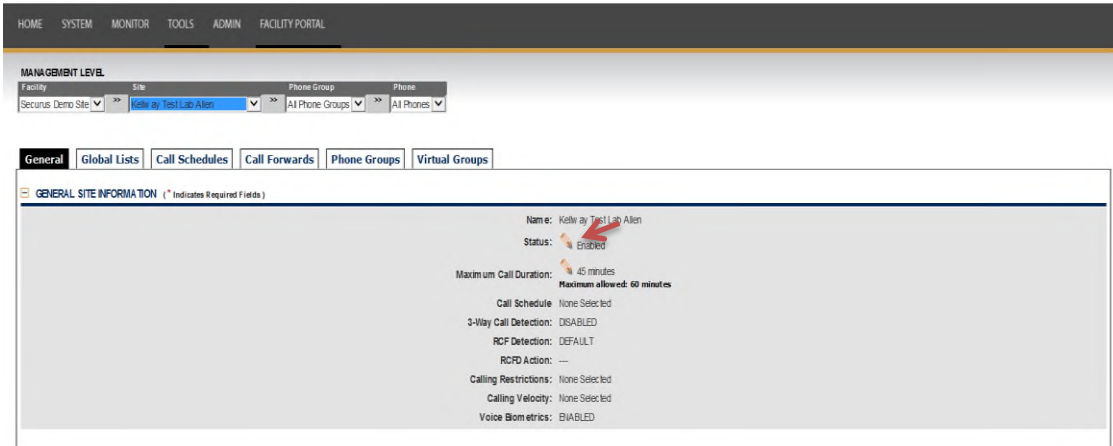
The power to shut down phones in any of the aforementioned manners is role based. Only personnel who have been given the proper authority through the security templates of SCP will be able to shut down phones. These security templates can be managed at a site level so only specific authorized staff at that site can manage those phones.

Also, authorized TDCJ personnel at Department headquarters will continue to have remote access and privileges to shut down the system at individual device up to a full facility level.

On/Off Station Control

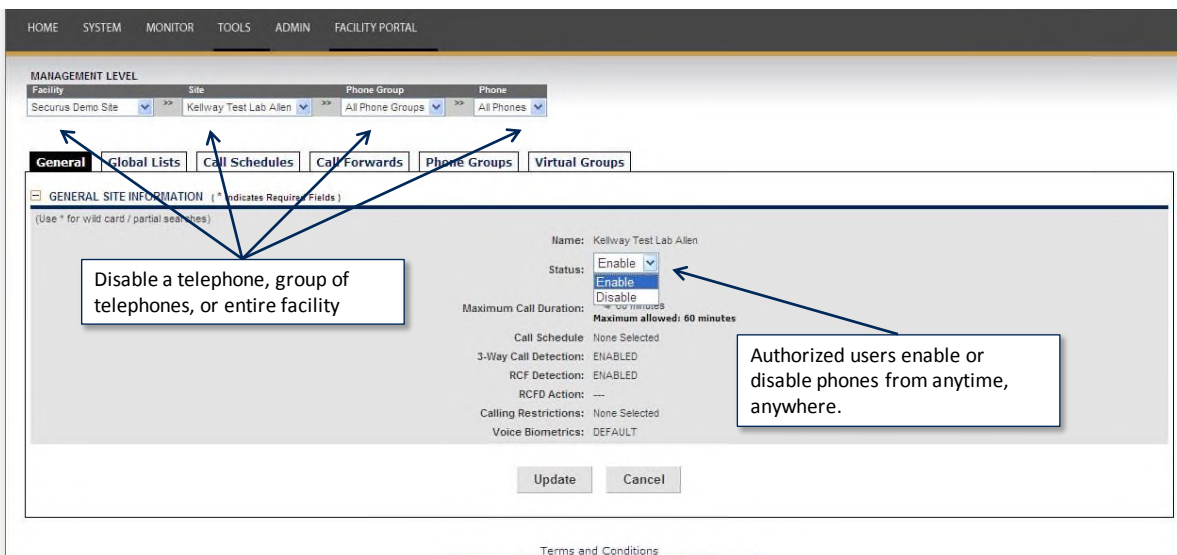
The OTS system will allow authorized Department personnel to immediately disable a telephone/terminal, a group of telephones/terminals, or an entire facility through the SCP portal from any workstation or mobile device with access to the internet. Securus is one of the only providers to offer this capability anytime, from anywhere, 24 hours a day, seven days a week.

To disable the phones, an authorized user would simply sign onto the SCP portal and from the System tab chose the site whose phones they would like to disable and/or the phone or group of phones. Once this is chosen, the user clicks on the pencil icon next to “status.”



After clicking on this icon, a drop box will appear providing the option to disable the selected phones. This modification tab provides options to the user to shut down the system in either “hard” or “soft” mode. Use of the “hard” mode cuts the call off immediately and shuts down the system. Soft mode allows the current conversation (if in progress) to continue to completion, then shuts the system off and does not allow another call to go through.

Disabling Telephones



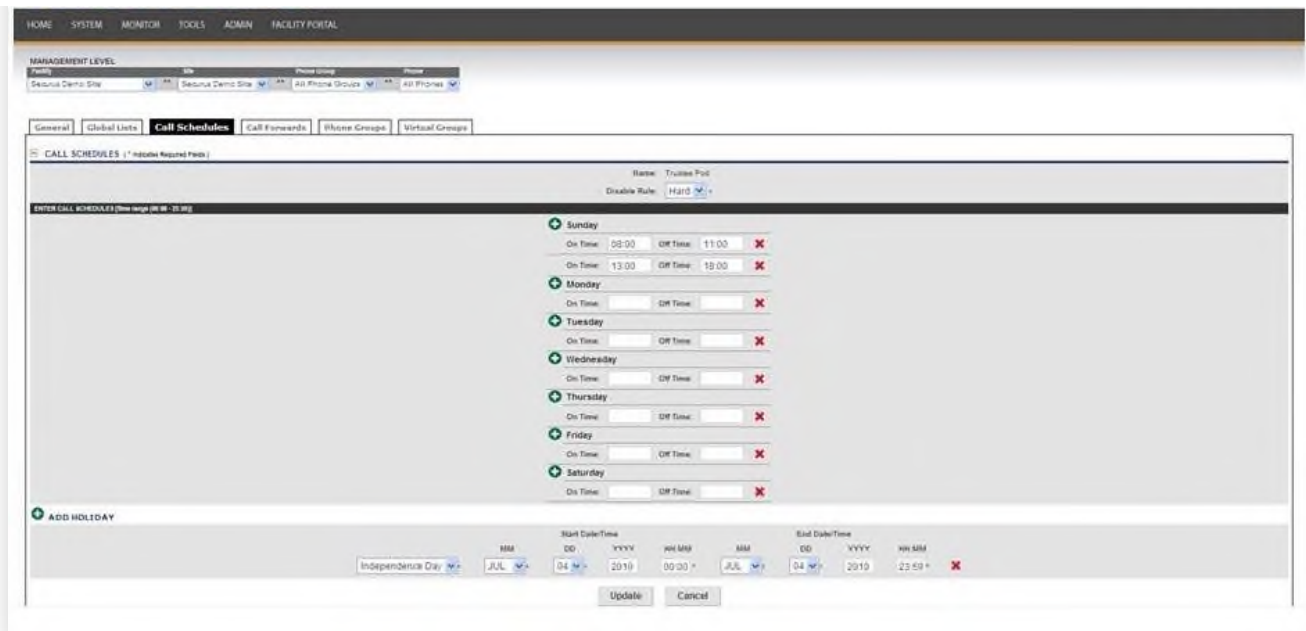
Programmable Calling Schedules

SCP also has automated calling schedules which allows the system to manage the scheduling policies of the facility without staff intervention. Calling schedules are used to turn on and off the phones during designated times throughout the day or night.

Calling schedules are flexible and configurable allowing the facility to have multiple on and off times during the day, within a week and by day of the week and then be applied to individual telephones, groups of telephones, individual offenders and/or globally.

Also, holiday overrides can be preset to accommodate anticipated exceptions to the set schedule.

Programming Calling Schedules



The screenshot displays the 'CALL SCHEDULES' configuration page. At the top, there are navigation tabs: 'General', 'Global Lists', 'Call Schedules', 'Call Forwards', 'Phone Groups', and 'Virtual Groups'. The 'Call Schedules' tab is active. Below the tabs, there's a section for 'CALL SCHEDULES (1* includes Required Fields)'. The main area shows a table for configuring calling schedules for each day of the week. The 'On Time' and 'Off Time' fields are populated with values like 08:00 and 11:00 for Sunday. There is also an 'ADD HOLIDAY' section at the bottom with a date picker.

7. **Proposer shall describe in detail, the format, media and method required to populate the Offender database as well as method(s) to update, edit, add, delete, suspend, reactivate, etc., records after the initial database is populated (Section C.3.1.1.D)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY



Advantage

The CenturyLink Team has already designed, developed, tested and implemented the necessary integrations for TDCJ. We will continue to use those integrations to provide TDCJ uninterrupted service while saving time during implementation.

The CenturyLink Team will be responsible for populating and maintaining accurate and up-to-date databases for the OTS. This includes ensuring that updates, edits, additions, deletions, suspensions, reactivations, etc. are populated. We will continue to provide all necessary tools, up to and including staff, computers, software, hardware, documents, printers, scanners, forms, test and accept equipment, training materials, and trainers, as detailed in our bid response. We will continue to be responsible for data entry and programming related to the databases for the term of the contract.

Although the transfer of data is all done automatically, an authorized user could have the capability to manually update, edit add, delete suspend, or reactivate a record.

We have an established interface with the Department that provides a current roster on a daily basis. This occurs through a database extraction in CSV format via SFTP.

The E-imports function within SCP then takes the transmitted information and populates the appropriate fields within the SCP system without further intervention from TDCJ staff.

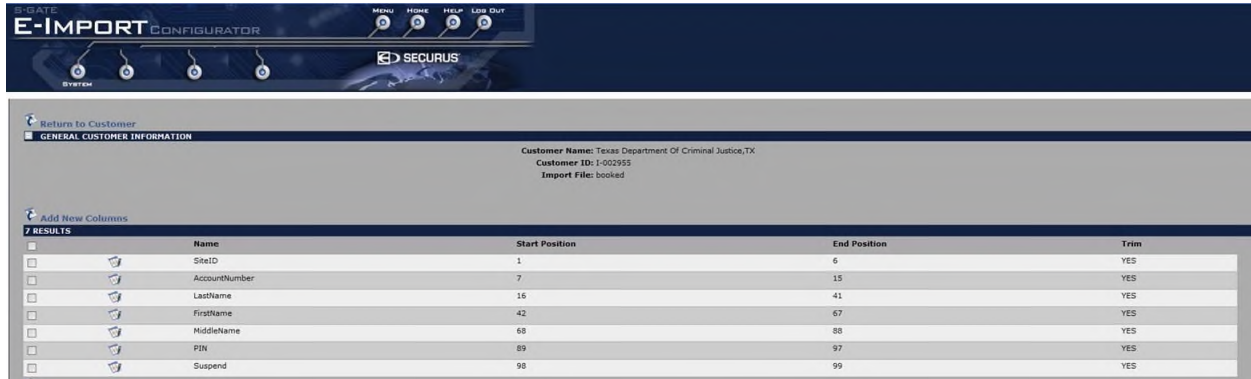
E-Imports: The E-imports application uploads data sent from the OMS into SCP, eliminating the need for facility personnel to enter offender information into the telephone system. E-imports updates offender profile information daily, such as intakes, transfers suspensions, etc.

The files that we currently receive from TDCJ through this integration include:

- Booked Files - Received Daily in order to create/reactivate offender accounts, update facility/PIN and manage activation/deactivation of suspensions.
- Complete File of All Offenders and their Current Status – Performed Monthly to ensure all offender files are the most up to date.
- Release Files - Received daily and automatically deactivates offender accounts as offenders are released from TDCJ.
- Change Account – Received weekly, providing information for changed offender account numbers and updating the system automatically.
- Debit File – Received daily providing commissary purchase information in order to update the debit account.

The Booked, Complete and Release files transmit the information to include the following fields.

- SiteID
- Account Number
- Last Name, First Name
- Middle Name
- PIN
- Suspension status.



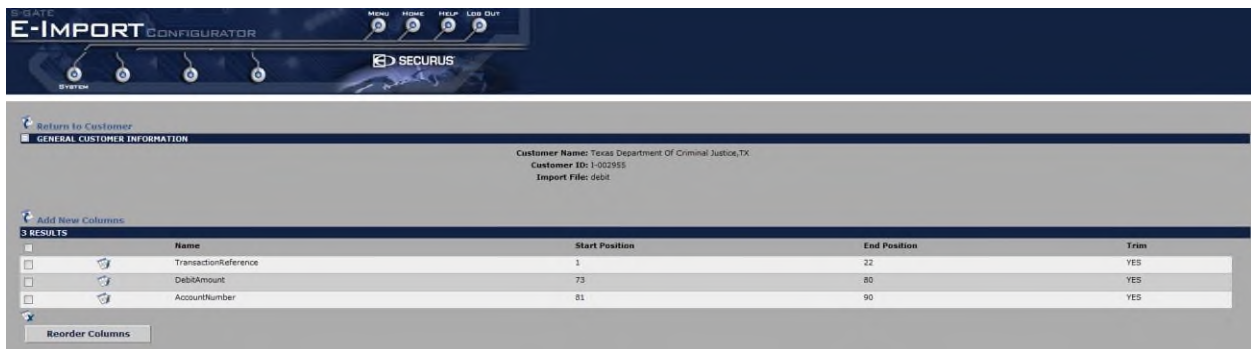
E-IMPORT CONFIGURATOR

Customer Name: Texas Department Of Criminal Justice, TX
 Customer ID: 1-002955
 Import File: booked

Name	Start Position	End Position	Trim
SiteID	1	6	YES
AccountNumber	7	15	YES
LastName	16	41	YES
FirstName	42	67	YES
MiddleName	68	88	YES
PIN	89	97	YES
Suspend	98	99	YES

The debit file transmits the information to include the following fields.

- Transaction Reference Number
- Debit Amount
- Offender's Account Number



E-IMPORT CONFIGURATOR

Customer Name: Texas Department Of Criminal Justice, TX
 Customer ID: 1-002955
 Import File: debit

Name	Start Position	End Position	Trim
TransactionReference	1	22	YES
DebitAmount	73	80	YES
AccountNumber	81	90	YES

The Change Account transmits the information to include the following fields.

- Old Account Number
- New Account Number



The screenshot shows the 'E-IMPORT CONFIGURATOR' interface. At the top, there are navigation buttons for 'MENU', 'HOME', 'HELP', and 'LOG OUT'. Below this, there's a 'GENERAL CUSTOMER INFORMATION' section with details for 'Texas Department Of Criminal Justice, TX'. The main part of the screenshot is a table with the following data:

Name	Start Position	End Position	Trim
OldAccountNumber	N/A	N/A	YES
AccountNumber	N/A	N/A	YES

8. **Proposer shall describe in detail, PBI and PIN features and functions of the proposed OTS and the method and format that will be used for PBI collection and PIN enrollment and updates to the OTS. (Section C.3.1.1.D)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The CenturyLink Team currently provides the Department with a voice print verification solution for the Personal Biometric Identifier (PBI). Securus' Voice Biometrics solution uses a proprietary voice print algorithm. **These PBIs will continue under the new contract without the need to re-enroll the existing offender population.**



The Voice Biometrics technology does not require special hardware. Instead, as a network-based solution it eliminates the risks of offender tampering and repeated on-premise repair of PBI systems such as fingerprint readers or retinal scanners.

Call progression with Voice Biometrics

When offenders place a call from the facility, they must first key in the language of the OTS system they want to use. After the language is selected, the offender will then be asked how they wish to fund the call (Debit or Collect). Once a payment option is selected, the offender will be asked to enter their PIN. If an invalid PIN is entered, the OTS will notify the offender of the invalid PIN status. After a successful PIN validation, the OTS system will prompt offenders to enter the phone number they wish to call. If the number is on the offender's authorized calling list, the voice biometric verification process will begin and the offender will be prompted to verify their name. Once the offender's name is validated, the call progresses to the next level of voice biometric verification. The offender will then be asked to say "Texas Department of Criminal Justice". If both voice biometric verifications are approved, the call will proceed. If the verification is not approved, the offender will receive a message stating that the voice was not verified and the call will end, forcing the offender to start a new, fully-controlled call.

The CenturyLink Team is responsible for the ongoing implementation of the database information of the OTS.

Implementation of PINs

The Department will provide a data file of every offender containing offender's First name, Last Name, Middle Name, offender site/unit ID, offender PIN, offender account number, and the offender suspension status. This information is currently uploaded into the OTS database through the e-imports application on a daily basis. We will continue to use this process and the same restrictions and policies will be implemented under any new contract.

Ongoing Implementation for Newly Processed Offenders

As the Department receives new offenders on an ongoing basis at specified intake facilities, we will continue to provide dedicated full-time Service Representatives located in close proximity to each intake facility to supervise enrollments for these new offenders. Additionally, as part of implementation of a new contract, the CenturyLink Team will make sure to enroll any offenders not currently in the system. The draft implementation plan found in Attachment F - Preliminary Implementation Plan, details the locations, dates and estimated duration to complete PBI enrollment, if necessary.

We recommend that enrollments take place at specified, mutually agreed-upon times during the week, thus minimizing the need for scheduling coordination with the Department. CenturyLink representatives verify offenders' identification numbers against the OTS database and enroll new offenders as needed.

Past experience dictates that offenders will try to manipulate the system if the enrollment is not supervised by an onsite team member. Not only will a supervised enrollment guarantee a clean capture of the offender's voice print, it will also expedite the enrollment process.

The database containing offender names and PIN's is used by onsite team members responsible for supervised enrollment of the offender's personal voice print.

The onsite enrollment personnel explain enrollment instructions to the offenders to ensure that each offender's enrollment is secure, accurate and successful

Enrollment Process:

1. Onsite team member will be located in the Day Room with a database of offender names and PIN's by facility or housing unit.
2. Team member will explain the process, hand them mail inserts to send to their Friends and Family and give them a brochure that explains the rules and answer basic questions.
3. Offender will give their full name and PIN and show their Department issued ID Card.
4. Team member will verify offender name and PIN against Department issued ID card
5. Offender will be instructed to remove all objects from their mouth, stand up straight and speak loud and clear
6. Offender is instructed that the OTS will prompt them to say their full name (first and last) three different times and they must pause between saying their first name and last name; the system will then prompt them to say "Texas Department of Criminal Justice" three different times; then the system will prompt them to verify their name.
7. Onsite team member will enter the offender PIN and then hand the telephone to the offender

8. System asks offender to state their full name at the tone
9. System prompts offender for name three times
10. System asks offender to say Texas Department of Criminal Justice at the tone
11. System prompts offender for facility name three times
12. System prompts them to verify their name
13. After name is verified, offender hears the system say thank you - goodbye
14. Team member tells the offender to hang up the phone
15. Enrollment is complete

Ongoing Implementation and Updates to PBI (Voice Biometrics)

In the unlikely event that an eligible offender must re-enroll or update his/her voice print PBI, the offender will submit an Assistance Request Form at the Unit's Mail Room. Those Assistance Request Forms are scanned in to the eMessaging system and delivered to the CenturyLink Team dedicated support team. A service ticket will be opened to ensure the issue is tracked and successful closure to the event. The resolution will include resetting the offender's voice prints and scheduling a new supervised re-enrollment into the voice biometric system.

9. **Proposer shall describe in detail the number of telephone numbers that can be stored by PBI and PIN for each Offender as well as the authorization process to add, remove, and validate a telephone number based on the Offenders approved call list. (C.3.1.1. D)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The OTS inherently supports this requirement. The OTS is completely programmable to support virtually unlimited combinations of allowed numbers by PIN/PBI. It is currently configured to allow 20 numbers by PIN/PBI.

Addition and Validation Process:

To have numbers added to an offender's PAN (Personal Allowed Number) list, the owner of the phone number must register their phone number at www.texasprisonphone.com or call the CenturyLink Registration Office at 866-806-7804. This is part of a rigorous process we have developed throughout the years, as described in Questions 39-40. Before the registration process is complete and the number is added to the offender's PAN list. TDCJ gives the final authorization for the number to be added.

Remove Process:

If an offender would like to remove an approved phone number from their PAN list, they can submit an Assistance Request Form at the unit's mail room. Those Assistance Request Forms are scanned in to the eMessaging system and delivered to the CenturyLink Team dedicated support team. A service ticket will be opened to ensure the request is tracked and successful closure to the event. The resolution will include deactivating the phone number from the offender's PAN list.

10. **Proposer shall clearly identify and delineate access control for each level and groups of levels, to include the correlated administrative/system capabilities of each level. Proposer shall indicate what, if any, flexibility is available to Department staff to modify or customize access levels. (Section C.3.1.1.E)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The SCP provides an advanced, multi-level password scheme that allows facility administrators to assign unique access levels to anyone using the different features of the SCP. Further, authorized users can assign specific capabilities to each access level through the security templates. The administrator may modify initial access levels or create additional levels based on facility objectives for each tool.

With SCP, Department personnel have the ability to access the system from any designated location, remote or otherwise, to perform tasks that correlate to the capabilities assigned to them through the security templates.

Password Standards

The SCP portal requires the following password standards to be utilized:

- The user ID jsmith@tdotx.tx is used to determine that the individual is authorized to only access applications determined to meet the appropriate clearance level
- For security purposes the system can also be configured to require a user password be updated/changed every 30/60/90 days or as required by the Department
- The user ID can be constructed using the user's first initial and last name or any combination authorized by the facility to create a unique user ID
- The user's password must be 4 – 14 characters in length, with at least one upper case letter and one numeric character, and must not contain spaces or blanks. Special characters are permitted
- The system can also be configured not to allow users to reuse previously used passwords

The current SCP password requirements in use today at TDCJ include the following:

- Minimum Length – 8
- Maximum Length – 14
- Expires every 30 days
- Cannot use the last 12 passwords

The TDCJ benefits significantly from the flexibility and configurability designed into the SCP. The TDCJ currently has over 900 active authorized users and created more than 30 unique TDCJ security templates for access control.

The CenturyLink team will ensure continued use of these templates and the continued flexibility to create new ones.

Security Templates

The following pages provide a brief description of the user profile settings within SCP. This document is intended to serve as a guide only and is not intended to define any particular roles within the TDCJ operations.

The OTS is completely configurable and can sustain as many roles (user types) to meet the Department's requirements. The standard User Profiles that are pre-configured into each customer's roles are depicted below. The Administrator Role is designed in a way that would normally be assigned to only one or two persons within the Department. This aids in controlling who can or cannot create new users, expand user's capabilities, change Department telephone policy (telephone schedules), add, change or delete security templates, and so on.

[Return to Template List](#)

TEMPLATE CREATED		
Name: Administrator		
Description: Administrator Role		
CONTROLLED AREA	CAN VIEW	CAN CHANGE
Admin - Recording Logs	✓	✓
Admin - Security Templates	✓	✓
Admin - User Management	✓	✓
Covert Alerts - View/Edit All Covert Alert	✓	✓
Covert Alerts - View/Edit Own Covert Alert	✓	✓
Monitor - Forward Call	✓	✓
Monitor - Listen to Live Calls and Recordings	✓	✓
Monitor - Terminate Call Monitor	✓	✓
Monitor - Terminate Monitored Calls	✓	✓
Monitor - View Live Calls	✓	✓
Report - Blocked Call Detail	✓	
Report - Call Detail	✓	✓
Report - Call Detail (All Access)	✓	✓
Report - Call Frequency	✓	✓
Report - Covert Alert Report	✓	✓
Report - Covert Alert Report (All Access)	✓	✓
Report - Hourly Usage	✓	✓
Report - Informant Line Call CDR Report		
Report - PAN Frequency (All Access)	✓	
Report - PAN Frequency Detail (All Access)	✓	
System - Call Forward List Administration	✓	✓
System - Call Party Accounts	✓	✓
System - Call Schedules	✓	✓
System - Global Lists	✓	✓
System - Global Lists (All Access)	✓	✓
System - Informant Line Call Global List		
System - Phone Config	✓	✓
System - Phone Group Config	✓	✓
System - Site Config	✓	✓
System - Velocity Restrictions	✓	✓

This is a list of the capabilities allowed within the Administrator Role. The preceding list also shows all the configurable items for a security template. On the following pages, each item is given a summary description.

Admin - Recording Logs

This security setting allows users with full Administrator rights to access, search, and view the Recording Logs for a specific user or view summary details of the activities performed by each user login account.

Admin - Security Templates

Site administrators use Security Templates to create new user security profiles. They can view, read, and modify current security templates to control a user's access to specific features and functions within the SCP user interface. Please note that users and administrators cannot modify profile templates that come standard with the system.

Admin - User Management

The User Management security setting allows authorized users to manage other users. This includes assigning new profiles on the SCP user interface, updating or deactivating users who no longer have access to the system, resetting passwords, and creating and modifying user accounts, including the sites a user can access at the customer level.

Covert Alerts - View/Edit All Covert Alert

The Covert Alerts View/Edit All Covert Alert security setting allows authorized users to view, edit, and modify any covert alert set in the system, and can override an existing covert alert created by another user.

Covert Alerts - View/Edit Own Covert Alert

The Covert Alerts View/Edit Own Covert Alert security setting allows authorized users to view, edit, and modify a covert alert if one does not yet exist and only if the user initially created the covert alert.

Monitor - Forward Call

This security setting allows authorized users with monitoring capabilities to forward a monitored call to another user who may be investigating the offender or the content of the call.

Monitor - Listen to Live Calls and Recordings

This security setting allows site administrators, investigators, and authorized personnel to monitor live calls in progress.

Monitor - Terminate Call Monitor

This security setting allows authorized users with monitoring capabilities to remotely terminate a call in progress.

Monitor - Terminate Monitored Calls

This security setting allows authorized users with monitoring capability to terminate a call in progress.

Monitor - View Live Calls

This security setting allows select users the ability to view only the list of live calls currently in progress for a site.

Report - Blocked Call Detail

The Blocked Call Detail security setting allows authorized users to have access to the blocked call detail report showing a listing by chosen criteria of all calls blocked for any reason.

Report - Call Detail

The Call Detail security setting allows select users access to the general view of a call detail report based on provided user criteria. A user granted access to this feature may not be able to view or access recording logs, listen to pre-recorded conversations or copy call recordings to a folder or download and burn calls to CD media

Report - Call Detail (All Access)

The Call Detail (All Access) security setting expands user capabilities beyond being able to query a CDR for the user-specified criteria. This setting allows authorized users full access to all elements of a call detail report including listening to associated call recordings, access to recording logs, copying and downloading calls to folders, and downloading call recordings to WAV files for burning to CD media.

Report - Call Frequency

The Call Frequency security setting provides authorized users access to a specified CDR report that can pull phone numbers meeting or exceeding a specified count. (Any phone number dialed more than two or three times or X number of times)

Report - Covert Alert Report

The Covert Alert security setting shows numbers connected to a covert alert.

Report - Covert Alert Report (All Access)

The Covert Alert (All Access) security setting show the numbers connected to a covert alert. It also provides the ability to listen to recordings within a call that was subject to a covert alert, access to the recording logs, copying and downloading calls to folders, and downloading call recordings to WAV files for burning to CD media.

Report - Hourly Usage

The Hourly Usage security setting allows authorized users to view a graphical display of phone usage. It also allows site administrators to verify their settings for calling times.

Informant Line Call CDR Report

This security setting allows authorized users to set up and configure the Informant Line, run, view and access all elements of the Informant Line Call Detail report including the list of calls by offenders to the Informant Line.

Report - PAN Frequency (All Access)

This security setting allows authorized users to run, view and have full access to a report listing the number of unique PINs/Offenders that have the same phone number on their PAN list.

Report - PAN Frequency Detail (All Access)

This security setting allows authorized users to run view and have full access to a report that produces a detailed list of offenders that share a number on their PAN list.

System - Call Forward List Administration

This security setting allows the user to create a list of individuals on his/her “Forward to Number;” this list appears when a user who is actively monitoring calls needs to forward a call for live monitoring.

Call Forward List Administration

This security setting allows authorized users to create a list of individuals on his/her “Forward to Number” list. This list appears when the user who is actively monitoring calls needs to forward a call for live monitoring.

System - Call Party Accounts

The Call Party Accounts (also known as Custody Accounts) security setting allows authorized users to manage custody accounts. This includes adding, modifying, and activating/deactivating a user’s phone account, or suspending a user’s phone access.

System - Call Schedules

This security setting allows authorized users to set up call schedules for a customer, a site, group of phones, or a single phone. These schedules automatically turn phones on and off per the prescribed schedule.

System - Global Lists

This security setting allows authorized users to view numbers on the global allow/block/watch list. Rules created under this section are applied site-wide unless created at the customer level; then it is applied to all sites under that customer.

System - Global Lists (All Access)

This security setting allows authorized users to view, edit, deactivate, or modify numbers on the global allow/block/watch list. Rules created under this section are applied site-wide, unless created at the customer level; then it is applied to all sites under that customer.

Informant Line Call Global List

This security setting allows authorized users to access, search, and view the Informant Line CDR on the Call Detail Report, and to search and view the summary of an Informant Line call from the Call Frequency Report.

System - Phone Config

This security setting allows authorized users to assign a phone to a Phone Group. Users may also assign special or unique call schedules or other parameters like Covert Alert. For example, a phone in the infirmary may be assigned to the phone group labeled “Medical.”

System - Phone Group Config

This security setting allows authorized users to specify the phones in a facility assigned to “groups.” These groups may have unique call schedules or other parameters. For example, phones labeled as “Medical Group” are the phones in the infirmary. Those phones are set to allow calls only from 3:00 PM to 6:00 PM, although the other phones at the site allow calls from 8:00 AM to 10:00 PM. Intake phones may be set to allow calls 24x7.

System - Site Config

This security setting allows authorized users to assign basic rules to a site. Some rules include maximum call duration, 3-way settings, or the call schedule under the customer profile.

Velocity Restrictions

This security setting allows authorized users read/write permission to the Velocity Restriction feature. A user with access to this feature can create new restriction policies or modify existing policies.

Note 1: By default, a user assigned to “Can Change” privilege must also be granted “Can View” privilege.

Note 2: Users cannot monitor, forward, or terminate Informant Line Calls because they are not displayed on the Live Monitoring Screen.

Flexibility for Department Staff to Modify

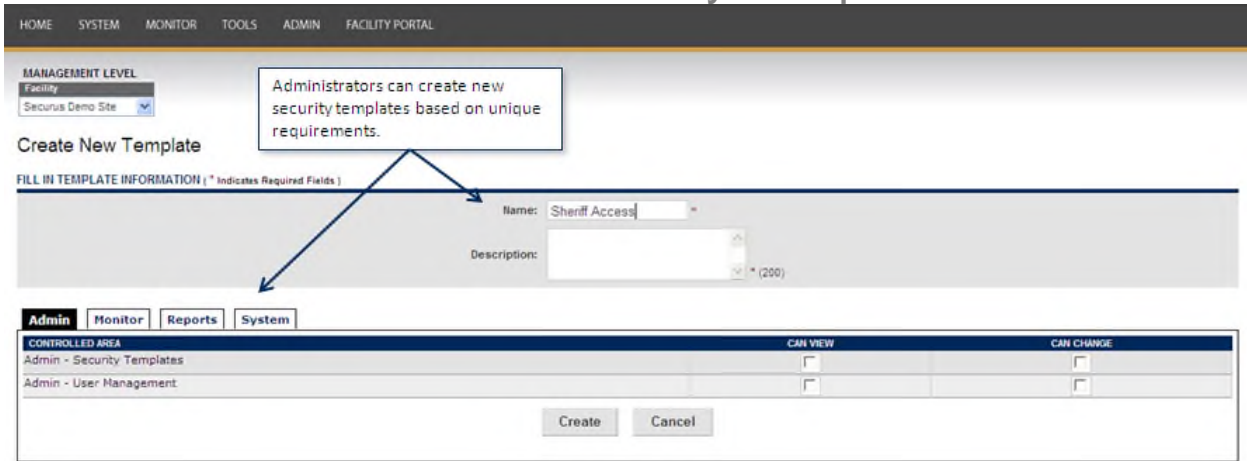
As mentioned above, the OTS is completely configurable. Therefore, if at any time the Department wants to modify the password standards set forth or modify and customize access levels, there are view and change options for each module depending on the need of the user.

Manage, Create, Edit, Predefine User Levels in SCP

NAME	DESCRIPTION	PREDEFINED
3rd Shift - blocking only	Night jailers can block number but no changes otherwise	
5.0 Huong test	Huong test	
5.0.1 Add Template	Huong Test	
5.1Huong Test	Huong test	
ADC-test1	This is for the demonstration	
ALL BUT NO 3 way	ALL permissions but no 3 way	
ALL BUT NO FREE	All but free	
Adam All	Everything	
Admin - Crime Tip Modify	Crime Tip Modify Access Admin	✓
Admin - Crime Tip Read	Crime Tip Read Access Admin	✓
Admin - Informant Line Modify	Informant Line Modify Access Admin	✓
Admin - Informant Line Read	Informant Line Read Access Admin	✓
Admin - No Monitor	Administrator w/o Live Monitoring Rights	✓

The administrator may modify the initial access levels or create additional levels based on facility clearance objectives for each tool. SCP generates a user log with the user name, time of access, and modules accessed.

Create New Security Templates

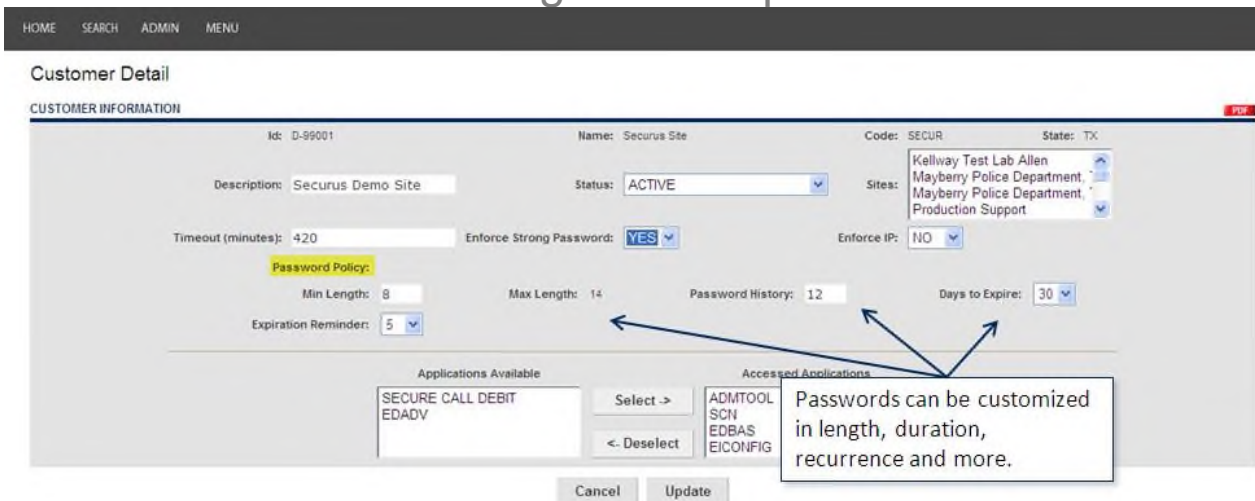


Additional Password Policy Options

We will continue to use the password standards that TDCJ has already set up for its users. However, SCP does provide flexible Password Policy options, enabling administrators to change their password requirements in the future if need be. Passwords can be configured by location, length, days to expire, and even the number of password cycles before password reuse. Additional configuration options include reminders for password expiration and minutes of allowable inactivity before session timeout.

If a user does not change their password before expiration, the user must contact the site administrator for password reset. This administrator assigns a random password and requires the user to create a new password when they log in.

Password Configuration Options in SCP



11. Proposer shall provide detailed explanation on how remote recording audio review is accomplished. (Section C.3.1.1.H)

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

Any authorized user with an approved user name and password can easily, and remotely, access recording and monitoring of offender 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

Live Call Monitoring

The SCP Live application allows for real-time monitoring of calls in progress using a secure connection from any internet connected device. 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 offender 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, offender 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 offender 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.

SCP writes all recorded calls to a Network Attached Storage array (NAS) in our primary Data Center. Each NAS array is also replicated to the secondary Data Center for redundancy and

failover. All recordings created on the platform reside in at least two of our Data Centers. Recordings are stored on-line for immediate access for the contractually agreed upon time. 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.

Recording Search and Retrieval

Users can specify search criteria, such as called party, calling telephone, date, time, PIN, custody account number, duration, and location, and 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 provide detailed information about each call and will indicate whether or not the call detail record (CDR) has an attached recording. If recorded, authorized investigators can listen to the recording using the embedded 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. While it is possible to make a recording from the speakers, this is only a copy of the original. 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.

Covert Alert

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

Covert Alert bridges a call to an authorized remote number for dialed numbers, phones, or offender 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 offender, 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 SCP 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, offender 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, offender PIN, originating telephone, dialed number, and an indication if the call has been recorded. The figure to the right provides a sample text message alert.

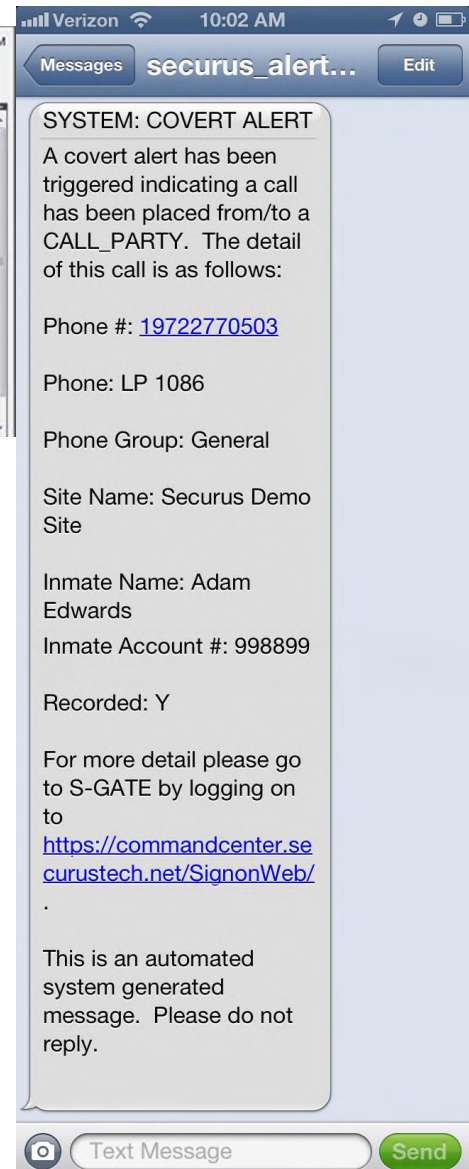
Additional Security Feature

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 offender at the TDCJ facility. 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 offender 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.



12. **Proposer shall describe in detail the types of adds, moves, and changes that can be made by Contractor staff and/or Department staff and the procedures required to add, move, and change records. Detail shall also include source records and method required to obtain Department records that correlates to the add, move, and change to be used as authorization and audit trail (e.g. Department downloads from mainframe databases). (Section C.3.1.1.F)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

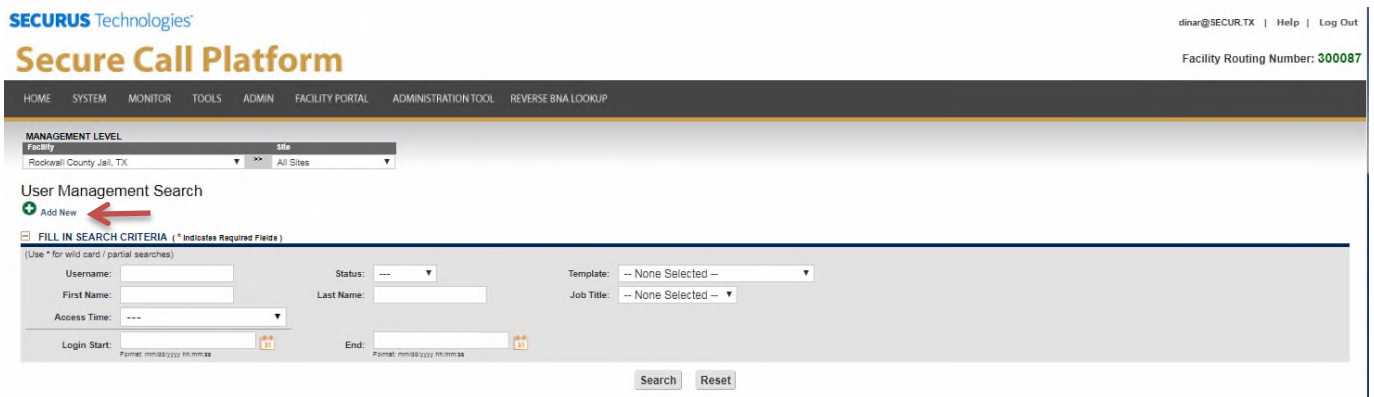
SCP was designed to be highly configurable to meet the needs of the Department. Adds moves and changes include those for authorized Department users and for offenders, as described in more detail below. All authorized adds, moves and changes are tracked within the system for auditing purposes.

Authorized User Add, Moves, and Changes

Management of authorized Department users occurs through the use of established user roles and security templates, which are developed and implemented by the CenturyLink Team in consultation with the Department. Today there are more than 30 customized, unique security templates in use at the Department. (e.g Office of Inspector General (OIG) Management, Information Technology Division (ITD) OTS, and Correctional Institution Division (CID) Level 1-6) New users are assigned these roles as they are entered into the system, based upon their job responsibilities.

Additions

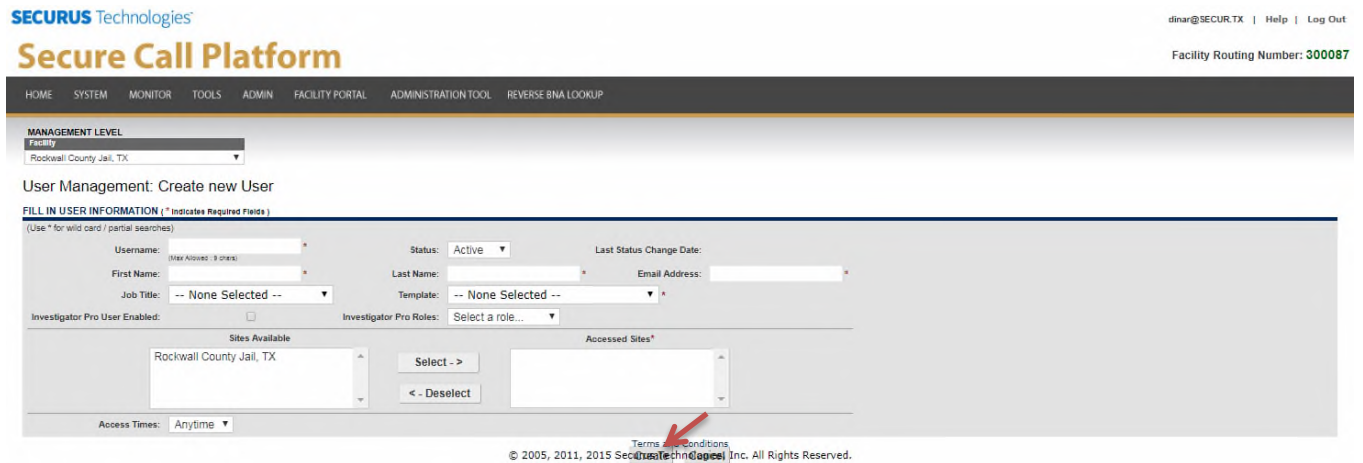
Authorized Department administrators can easily add a user to SCP through the “Admin” module by going to the User Management page. There is an “add new” button (see below) whereby clicking on it will open the User Management: Create new User Page.



To finalize the creation of a new user, the administrator must fill in the required fields as indicated by the red asterisk and click on the “create” button at the bottom of the page.

Required Fields:

- Username
- Status - This can be set as active or inactive.
- First and Last Name
- Job Title
- Template:
- Accessed Sites



Offender Add, Moves, and Changes

The CenturyLink Team will be responsible for populating and maintaining accurate and up-to-date offender data within the OTS. This includes ensuring that updates, edits, additions, deletions, suspensions, reactivations, etc. are populated. We will continue to provide all necessary tools, up to and including staff, computers, software, hardware, documents, printers, scanners, forms, test and accept equipment, training materials, and trainers, as detailed in our bid response. We will continue to be responsible for data entry and programming related to the databases for the term of the contract.

Although the transfer of data is all done automatically, an authorized user has the ability to manually update, edit add, delete suspend, or reactivate a record.

We have an established interface with the department that provides a current roster on a daily basis. This occurs through database extract in CSV format via SFTP. The E-imports function within SCP then takes transmitted information and populates the appropriate fields within the SCP system without further intervention from TDCJ staff.

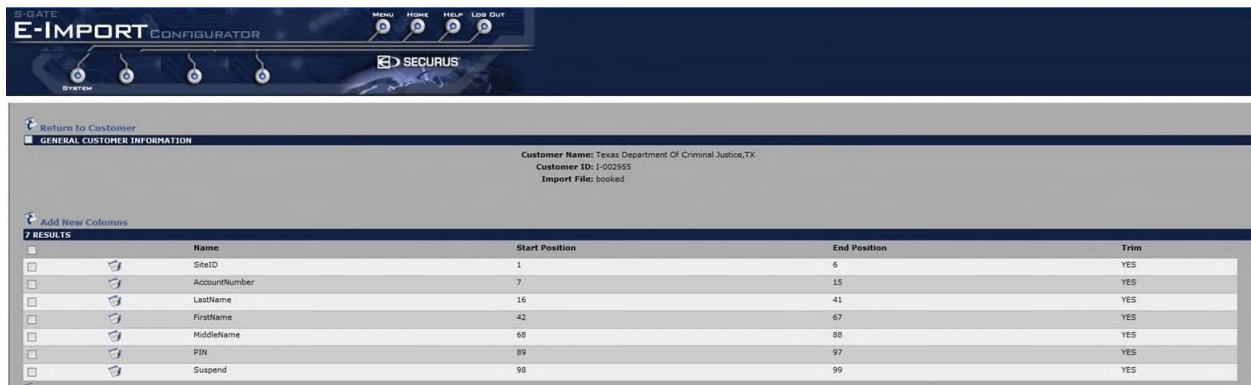
The files that we currently receive from TDCJ through this integration include:

- Intake Files - Received Daily in order to create/reactivate offender accounts, update facility/PIN and manage activation/deactivation of suspensions.
- Complete File of All Offenders and their Current Status – Performed Monthly to ensure all offender files are the most up to date.

- Release Files: Received daily and automatically deactivates offender accounts as offenders are released from TDCJ.
- Change Account – Received weekly, providing information for changed offender account numbers and updating the system automatically.
- Debit File – Received daily providing commissary purchase information in order to update the debit account.

The Intake, Complete and Release files transmit the information to include the following fields.

- SiteID
- Account Number
- Last Name, First Name
- Middle Name
- PIN
- Suspension status.

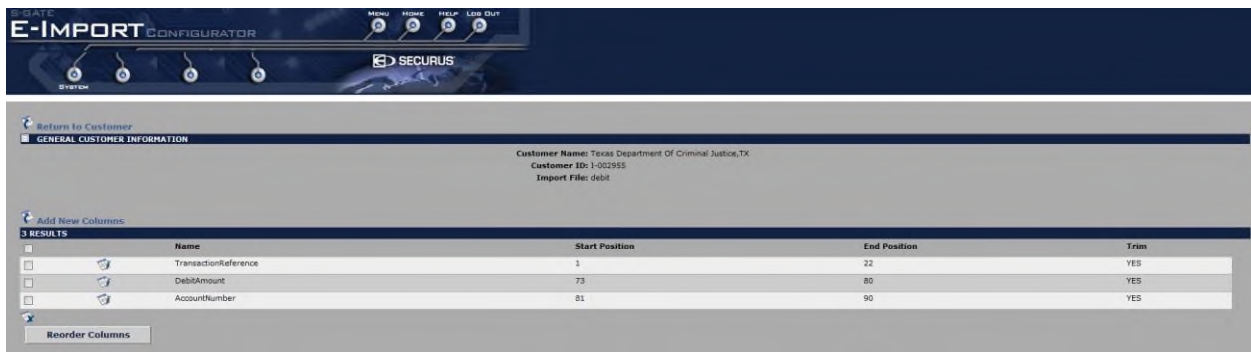


Customer Name: Texas Department Of Criminal Justice, TX
Customer ID: 1-002955
Import File: booked

Name	Start Position	End Position	Trim
SiteID	1	6	YES
AccountNumber	7	15	YES
LastName	16	41	YES
FirstName	42	67	YES
MiddleName	68	88	YES
PIN	89	97	YES
Suspend	98	99	YES

The debit file transmits the information to include the following fields.

- Transaction Reference Number
- Debit Amount
- Offender's Account Number



Customer Name: Texas Department Of Criminal Justice, TX
Customer ID: 1-002955
Import File: debit

Name	Start Position	End Position	Trim
TransactionReference	1	22	YES
DebitAmount	73	80	YES
AccountNumber	81	90	YES

The Change Account transmits the information to include the following fields.

- Old Account Number
- New Account Number



13. **Proposer shall describe in detail the procedures required for the Department to generate, order, or view any and all reports available via the proposed OTS. Proposer shall list in detail with full explanation the type of reports the proposed system can provide per facility as well as the method of presentation (on-line view, printable, real time, query, ad hoc, etc.). (Section C.3.1.1.G)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The system has a rich set of standard and ad-hoc reporting capabilities. In addition, the dedicated CenturyLink account team provides a number of customized reports – including all of those listed C.3.1.1.G – plus numerous other customized reports that have been developed specifically for TDCJ at the request of the Department staff.

Reports Available through SCP User Interface

The SCP portal is the single access point for all report generation. Like other web-based applications, screens are intuitive and have easy access to help through the click of a mouse. Users navigate to the information they are seeking topic by topic, or they can follow the table of contents for a complete training experience.

Reports are generated either on demand or on an ad hoc basis. OTS has the capability to produce reports on a scheduled basis and on demand. The OTS reporting system allows the originator of the report to view the information on-line, in printed format, via query, all in near real time. As an added benefit, all reports include the ability to export to Excel, PDF, or CSV formats. Further, the CenturyLink Team's dedicated Service Manager would always be available to help develop automated reports customized to the Department's needs.

The OTS has a dedicated reports writer that provides investigative information based on the Call Detail Records (CDRs). This sophisticated reporting tool can provide routine scheduled reports, or reports on an ad hoc basis. The OTS is capable of searches and call detail analysis on all calls, sorted by offender telephone location, destination number, time and duration, PIN, and much more. Call details are kept on all call attempts, except those to blocked numbers. However, view access to different types of CDRs (for example, calls to crime tips lines) can be restricted by individual user level.

The OTS provides standard reports with parameter fields that allow the user to define the information content of each report:

- 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 application compiles the data and displays the information in a report format, on the workstation monitor, in a matter of seconds regardless of the volume of information retrieved. Further, this application provides multiple functions for call playback, copying calls to remote media and restoring calls from an archival mode. There are virtually no limits to the type of information available through Investigative Reports.

Below is a sampling of reports available through the SCP portal. Please refer to Attachment H – Sample SCP Reports.

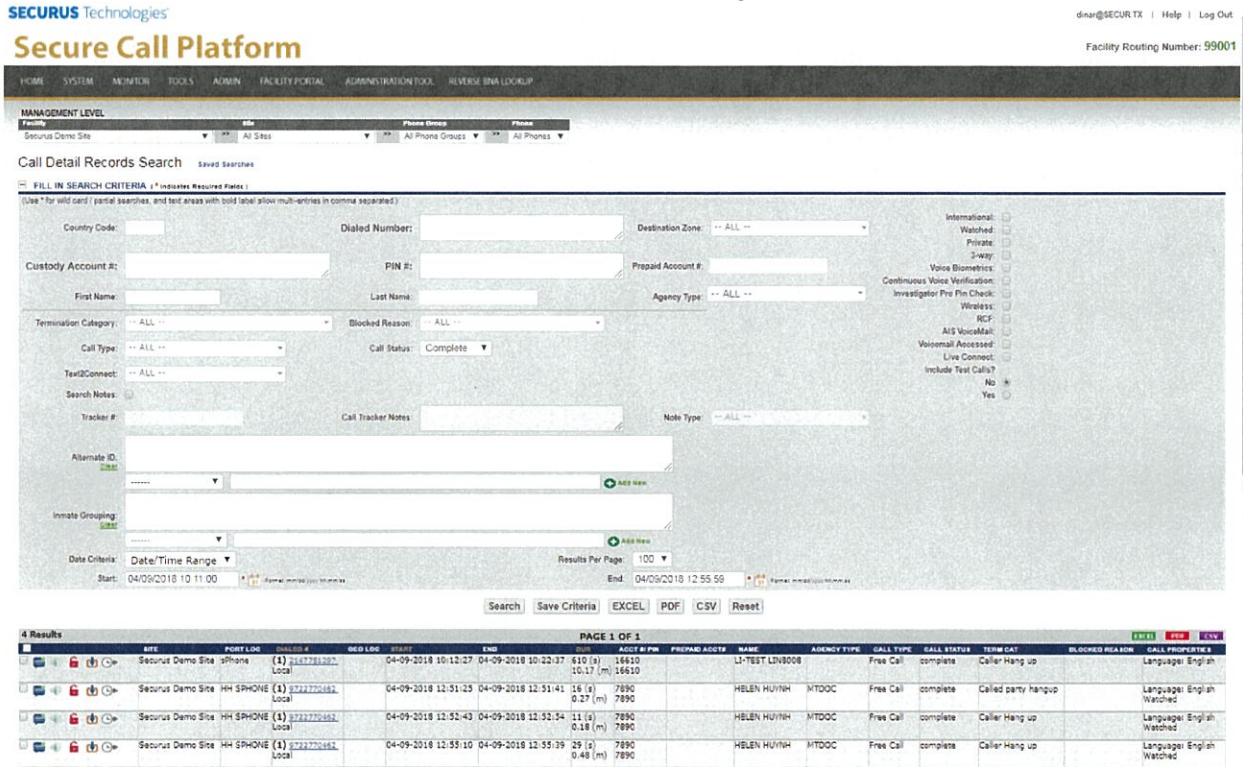
Call Detail Report

The Call Detail Report (CDR) provides investigators an intuitive and user-friendly report to view or search virtually anything related to an offender 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
- 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
- Desired results per page

Call Detail Report



SECURUS Technologies
Secure Call Platform

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL ADMINISTRATION TOOL REVERSE 911 LOOKUP

MANAGEMENT LEVEL: Securus Demo Site

Call Detail Records Search

SEARCH CRITERIA: Country Code, Dialed Number, Destination Zone, Custody Account #, PIN #, Prepaid Account #, First Name, Last Name, Agency Type, Termination Category, Blocked Reason, Call Type, Call Status, TextConnect, Search Notes, Tracker #, Call Tracker Notes, Note Type, Alternate ID, Inmate Grouping, Date Criteria, Results Per Page.

4 Results

SITE	PORT/LIN	PHONED #	REQ LOG	START	END	RESULTS PER PAGE	PROVIDER	NAME	AGENCY TYPE	CALL TYPE	CALL STATUS	TERMINAT	BLOCKED REASON	CALL PROPERTIES
Securus Demo Site	9PHONE	(1) 2147771051	Local	04-09-2018 10:12:27	04-09-2018 10:22:37	610 (a) 10.17 (m)	14610	L1-TEST LTN8008		Free Call	complete	Caller Hang up		Language: English Watched
Securus Demo Site	HH 9PHONE	(1) 9727701682	Local	04-09-2018 12:51:23	04-09-2018 12:51:41	16 (s) 0.27 (m)	7890	HELEN HUYNH	MTDOC	Free Call	complete	Called party hangup		Language: English Watched
Securus Demo Site	HH 9PHONE	(1) 9727701682	Local	04-09-2018 12:52:43	04-09-2018 12:52:54	11 (s) 0.18 (m)	7890	HELEN HUYNH	MTDOC	Free Call	complete	Caller Hang up		Language: English Watched
Securus Demo Site	HH 9PHONE	(1) 9727701682	Local	04-09-2018 12:55:10	04-09-2018 12:55:39	29 (s) 0.48 (m)	7890	HELEN HUYNH	MTDOC	Free Call	complete	Caller Hang up		Language: English Watched

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

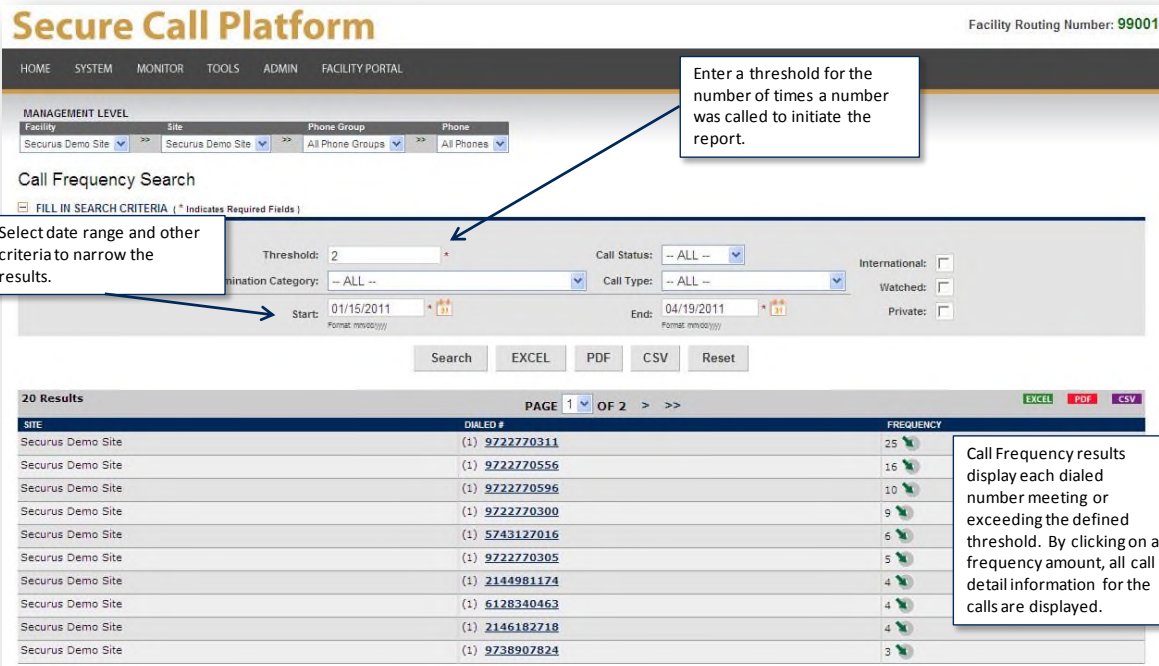
- Add notes to a call record or a tracking number
- Mark the notes private or public
- Play the call
- Copy the call to a management folder for download
- Download the call immediately with a one click operation
- Extend the call expiration date if it is approaching the agreed upon storage threshold
- 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 Frequency Report



Secure Call Platform Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Facility	Site	Phone Group	Phone
Securus Demo Site	Securus Demo Site	All Phone Groups	All Phones

Call Frequency Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

Threshold: 2

Call Status: -- ALL --

International:

Termination Category: -- ALL --

Call Type: -- ALL --

Watched:

Private:

Start: 01/15/2011

End: 04/19/2011

Search EXCEL PDF CSV Reset

20 Results PAGE 1 OF 2

SITE	DIALED #	FREQUENCY
Securus Demo Site	(1) 9722770311	25
Securus Demo Site	(1) 9722770556	16
Securus Demo Site	(1) 9722770596	10
Securus Demo Site	(1) 9722770300	9
Securus Demo Site	(1) 5743127016	6
Securus Demo Site	(1) 9722770305	5
Securus Demo Site	(1) 2144981174	4
Securus Demo Site	(1) 6128340463	4
Securus Demo Site	(1) 2146182718	4
Securus Demo Site	(1) 9738907824	3

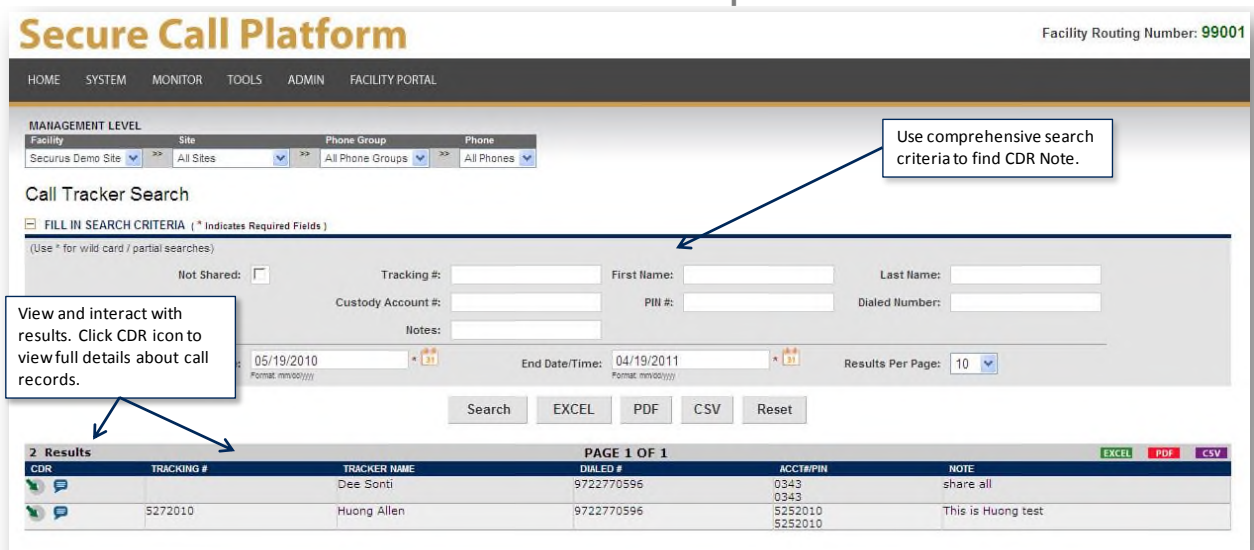
Call Frequency results display each dialed number meeting or exceeding the defined threshold. By clicking on a frequency amount, all call detail information for the calls are displayed.

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

Call Tracker Report



Secure Call Platform Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL
 Facility: Securus Demo Site Site: All Sites Phone Group: All Phone Groups Phone: All Phones

Call Tracker Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)
 (Use * for wild card / partial searches)

Not Shared: Tracking #: _____ First Name: _____ Last Name: _____
 Custody Account #: _____ PIN #: _____ Dialed Number: _____
 Notes: _____

05/19/2010 End Date/Time: 04/19/2011 Results Per Page: 10
Format: mm/dd/yyyy Format: mm/dd/yyyy

Search EXCEL PDF CSV Reset

2 Results PAGE 1 OF 1 EXCEL PDF CSV

CDR	TRACKING #	TRACKER NAME	DIALED #	ACCT/PIN	NOTE
		Dee Sonti	9722770596	0343 0343	share all
	5272010	Huong Allen	9722770596	5252010 5252010	This is Huong test

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)

Hourly Usage Report

Secure Call Platform
Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

Facility	Site	Phone Group	Phone
Securus Demo Site	All Sites	All Phone Groups	All Phones

Hourly Usage Report

FILL IN SEARCH CRITERIA (* Indicates Required Fields)
(Use * for wild card / partial searches)

Call Status: Complete

Date Criteria: Date/Time Range (Note: Date Range Search Criteria is restricted to 1 week)

Start: 04/20/2011 00:00:00 Format: mm/dd/yyyy hh:mm:ss

End: 04/25/2011 23:59:59 Format: mm/dd/yyyy hh:mm:ss

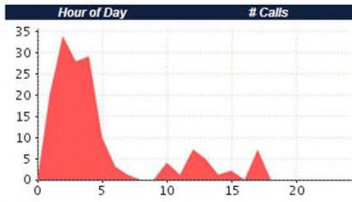
International:

Watched:

Private:

Search PDF Reset

Results PDF



Hour of Day **# Calls**

Hour	# Calls
00:00	0
01:00	20
02:00	34
03:00	28
04:00	29
05:00	10
06:00	3
07:00	1
08:00	0
09:00	0
10:00	4
11:00	1
12:00	7
13:00	5
14:00	1
15:00	2
16:00	0
17:00	7
18:00	0
19:00	0
20:00	0
21:00	0
22:00	0
23:00	0

Hourly Usage Report – is a valuable administrative report that displays the number of phone calls that have taken place within a given date and time range. Search criteria includes international, watched, private, call status, and date/time.

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

Covert Alert Call Detail Record Report

Secure Call Platform

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL ADMINISTRATION TOOL

MANAGEMENT LEVEL

Facility: Securus Demo Site | Site: All Sites | Phone Group: All Phone Groups | Phone: All Phones

Covert Alert Call Detail Records Search


FILL IN SEARCH CRITERIA (* Indicates Required Fields)

223 Results PAGE 1 OF 23 >

SITE	PORT LOC	ALERTEE DIALED #	ALERTEE NAME	TERM CAT	START						
Securus Demo Site	Princeton 4	214-558-4138	Kobe Bryant	No Investigator Acceptance	02-06-2017 10:00:40						
Securus Demo Site	Princeton 4	9036403050	derek Partridge	Parent Call Ended	02-06-2017 10:00:49						
Securus Demo Site	Princeton 4	9726329852	shana white	No Investigator Acceptance	02-06-2017 10:00:49						
Securus Demo Site	Princeton 4	9726329852	shana white	Parent Call Ended	02-06-2017 17:14:50						
Securus Demo Site	Princeton 4	9036403050	derek Partridge	Parent Call Ended	02-06-2017 17:14:50	02-06-2017 17:15:04	14	8179070658	JEH1001101162	Brenda Dodger	complete
Securus Demo Site	LP 16	6123804566	Tom Hoffman	System Failure Dialing Investigator	02-07-2017 23:23:40	02-07-2017 23:23:45	5	9722770379	03790379	Ken Burns	complete
Securus Demo Site	LP 16	6123804566	Tom Hoffman	System Failure Dialing Investigator	02-08-2017 00:14:06	02-08-2017 00:14:11	5	9722770379	03790379	Ken Burns	complete
Securus Demo Site	LP 16	6123804566	Tom Hoffman	System Failure Dialing Investigator	02-08-2017 00:26:42	02-08-2017 00:26:47	5	9722770379	03790379	Ken Burns	complete
Securus Demo Site	LP 16	6123804566	Tom Hoffman	System Failure Dialing Investigator	02-08-2017 00:35:55	02-08-2017 00:35:59	4	9722770379	6311	Ken Burns	complete

Covert Alert Report results display critical information about each triggered alert, such as; who was alerted, what happened, call status, call start and end, call duration, dialed number and more.

Clicking the icon next to each call record allows users to see the call detail information. SCP's Covert Alert feature and reports have assisted in many criminal investigations throughout the country.



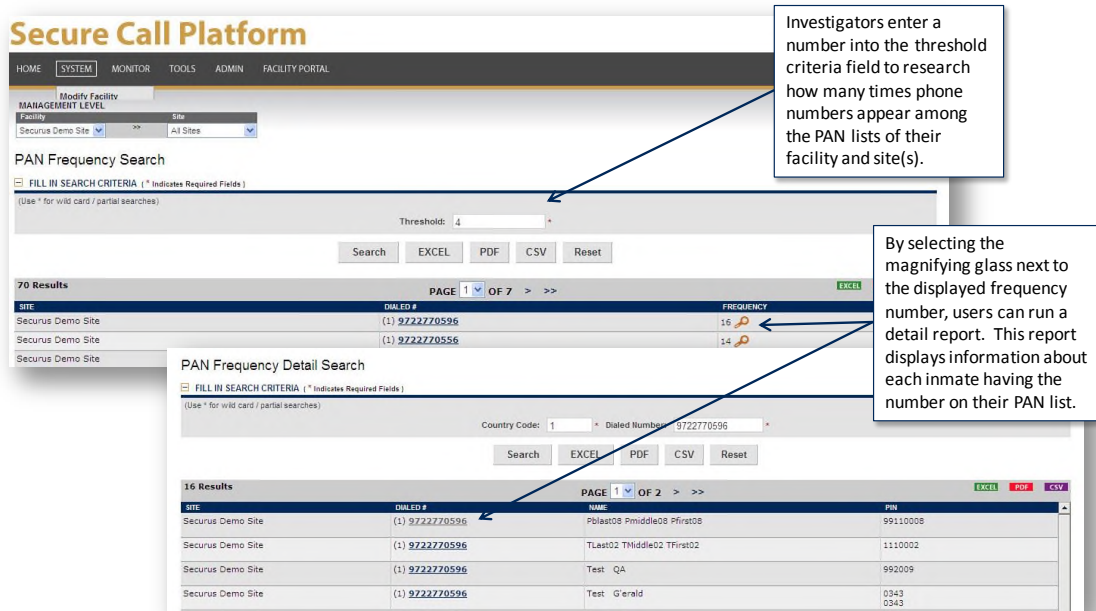
Personal Allowed Number Frequency Report

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.

Personal Allowed Number Frequency Report



Secure Call Platform

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

Modify Facility
MANAGEMENT LEVEL

Facility: Securus Demo Site Site: All Sites

PAN Frequency Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)
(Use * for wild card / partial searches)

Threshold: 4

Search EXCEL PDF CSV Reset

70 Results PAGE 1 OF 7

SITE	DIALED #	FREQUENCY
Securus Demo Site	(1) 9222770596	16
Securus Demo Site	(1) 9222770556	14
Securus Demo Site		
Securus Demo Site		

PAN Frequency Detail Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)
(Use * for wild card / partial searches)

Country Code: 1 Dialed Number: 9222770596

Search EXCEL PDF CSV Reset

16 Results PAGE 1 OF 2

SITE	DIALED #	NAME	PIN
Securus Demo Site	(1) 9222770596	Pblast08 Pmiddle08 Pfirst08	99110008
Securus Demo Site	(2) 9222770596	TLast02 TMiddle02 TFirst02	1110002
Securus Demo Site	(1) 9222770596	Test QA	992009
Securus Demo Site	(2) 9222770596	Test Gerald	0343 0343

Investigators enter a number into the threshold criteria field to research how many times phone numbers appear among the PAN lists of their facility and site(s).

By selecting the magnifying glass next to the displayed frequency number, users can run a detail report. This report displays information about each inmate having the number on their PAN list.

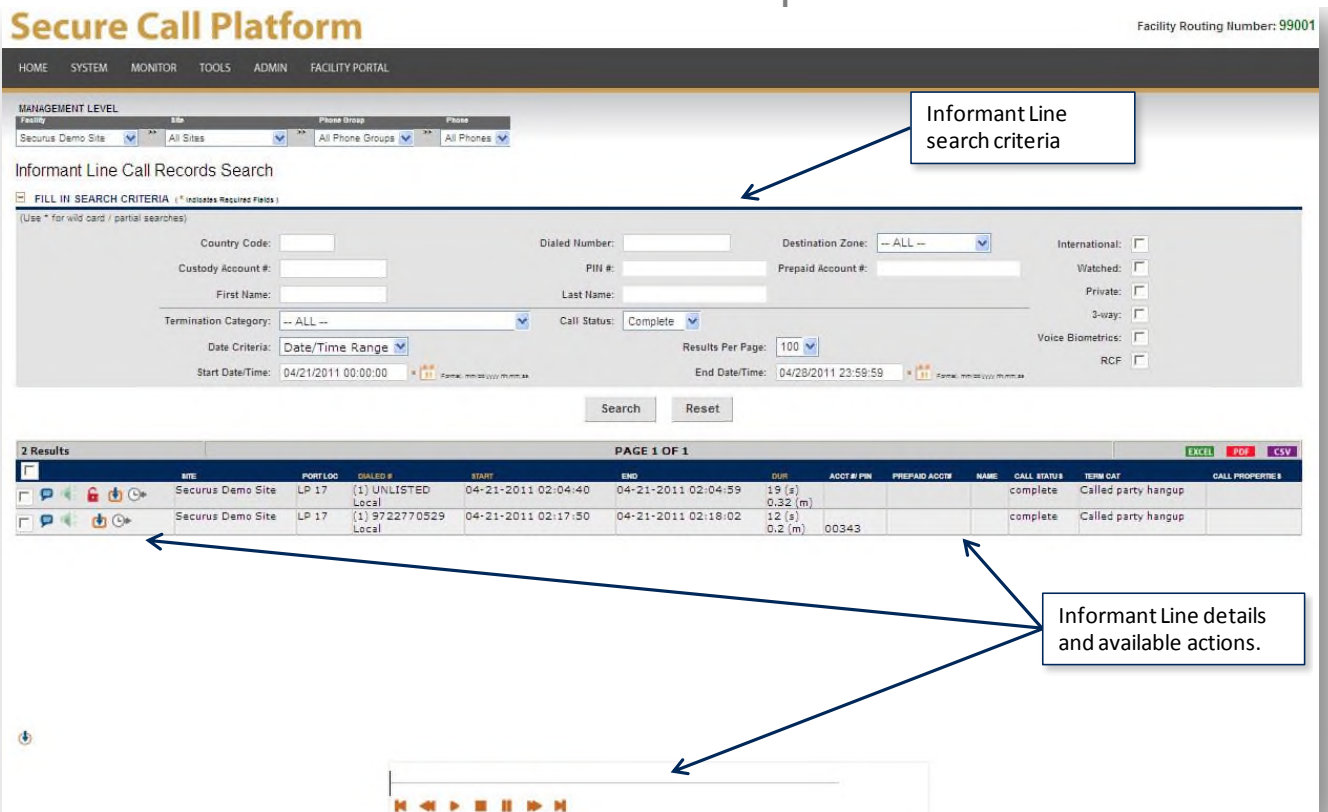
Informant Line Report

The Informant Line Report allows users to search for calls placed to the informant line and distinguish these calls from regular offender 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 Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Site: Securus Demo Site Phone Group: All Sites Phone: All Phone Groups All Phones

Informant Line Call Records Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches)

Country Code: [] Dialed Number: [] Destination Zone: -- ALL -- International:

Custody Account #: [] PIN #: [] Prepaid Account #: [] Watched:

First Name: [] Last Name: [] Private:

Termination Category: -- ALL -- Call Status: Complete 3-way:

Date Criteria: Date/Time Range Results Per Page: 100 Voice Biometrics:

Start Date/Time: 04/21/2011 00:00:00 End Date/Time: 04/28/2011 23:59:59 RCF:

Search Reset

2 Results PAGE 1 OF 1 EXCEL PDF CSV

	SITE	PORT LOG	DIALING #	START	END	DURATION	ACCT # / PIN	PREPAID ACCT#	NAME	CALL STATUS	TERM CAT	CALL PROPERTIES
<input type="checkbox"/>	Securus Demo Site	LP 17	(1) UNLISTED Local	04-21-2011 02:04:40	04-21-2011 02:04:59	19 (s) 0.32 (m)				complete	Called party hangup	
<input type="checkbox"/>	Securus Demo Site	LP 17	(1) 9722770529 Local	04-21-2011 02:17:50	04-21-2011 02:18:02	12 (s) 0.2 (m)	00343			complete	Called party hangup	

Call Log Navigation: [Home] [Previous] [Next] [End]

Informant Line search criteria

Informant Line details and available actions.

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 offender, for all offenders in a facility, or for all facilities

Secure Call Platform Debit Report

Secure Call Platform

By using the criteria in the search area, users can run reports detailing and totaling SCP Debit activity and balances for their facility.

HOME
SYSTEM
MONITOR
TOOLS
ADMIN
FACILITY PORTAL

MANAGEMENT LEVEL

Facility	Site	Phone Group	Phone
Securus Demo Site	All Sites	All Phone Groups	All Phones

SCP Debit Transaction Search
(Negative numbers will be displayed in parenthesis)

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches)

Inmate First Name: <input type="text"/>	Last Name: <input type="text"/>	Custody Account #: <input type="text"/>	PIN: <input type="text"/>
User Name: <input type="text"/>	User Comments: <input type="text"/>	Description: <input type="text"/>	
Type: <input type="text" value="--ALL--"/>	Amount: <input type="text" value="--ALL--"/>	Exclude Automated Process: <input checked="" type="checkbox"/>	

Note: Please limit search range to no more than 31 days

Start: <input type="text" value="06/15/2017 00:00:00"/>	End: <input type="text" value="07/10/2017 23:59:59"/>
---	---

1 of 2 ?
Select a format
Export

Site	Account # / PIN	Inmate First/Last	Type	Amount	Date/Time (In Central Time)	User	Reference #	Description	Comment
Securus Demo Site	6311 / 6311	KEN BURNS	Credit	\$50.00	06/28/2017 10:42:35	kburns@SECUR.T	20174228104235-6311	Site Issued Credit	test calls in Demo
Securus Demo Site	060827 / 060827	CHAN TRAN	Credit	\$200.00	06/27/2017 04:14:33	kburns@SECUR.T	20171427041432-060827	Site Issued Credit	Added for testing in Production
Securus Demo Site	6311 / 6311	KEN BURNS	Credit	\$15.00	06/27/2017 10:03:19	kburns@SECUR.T	20170327100319-6311	Site Issued Credit	Adding for testing Securus Demo
Securus Demo Site	0864 / 0864	CHUONG TEST	Credit	\$2.00	06/16/2017 03:28:33	gray2@SECUR.TX	S20170616152833147	Site Issued Credit	mt
TOTALS									
				Action Type	Quantity	Amount			
				Payment	0	\$0.00			
				Credit	4	\$267.00			
				Debit	0	\$0.00			
				4	\$267.00				

Reports Provided to the Department by the CenturyLink Account Team

The CenturyLink Team currently provides the Department with the Following reports:

- Fiscal Year Statistic Reports - Which include all of the details enumerated in Section C.1.1.G.
- Attorney Quarterly Audit
- New Workstation installation and activation report
- Annual Network Redundancy Testing Report

As we worked closely with the Department to create many of the contractor provided reports the Department is requesting, we are very adept in providing reports to TDCJ. We will continue

to submit these reports no later than the 20th of each month for the previous month and in the format that the CenturyLink Team and the Department agreed upon.

Enhanced Service Reporting

Immediately following the initial implementation of the OTS, CenturyLink worked closely with TDCJ to customize ongoing reporting. Subsequent to the initial implementation, TDCJ deployed numerous enhanced services including WCS, ICER, forensic lab, THREADS, call monitoring and IPRO. Following implementation of these enhanced services, CenturyLink again worked with TDCJ to customize reporting for those services listed below.

- **Wireless Containment System (WCS)** - Reporting of illegal contraband cell phone activity within TDCJ facilities that is provided to the OTS staff for review and follow up action. On demand, real-time, hourly, daily, weekly and monthly reporting is available.
- **ICER Reporting** – Daily reporting of illegal communication between TDCJ offenders or a TDCJ offender illegally communicating with offenders located in another jurisdictional facility such as Louisiana DOC, Harris County or Dallas County.
- **Forensic Lab** – Ad-hoc reporting provided to OIG staff of data extracted from contraband cells phones or other confiscated devices. Data is available in written report format in addition to extracted data being available within the THREADS analytical software.
- **THREADS** - Data analytics engine analyzes multiple types of Department data, such as offender communication records, public phone records, billing name and address, data from confiscated cell phones, financial data, and more to automatically generate on demand and regularly scheduled reports to TDCJ staff.
- **Call Monitoring** – Targeted call monitoring includes reporting to the OIG and CID of all gathered actionable intelligence upon discovery in agreed upon format and timeframe.
- **IPRO** – The Investigator Pro call player and reporting system allows for significant on-demand reporting of each and every call where an offender’s voice or targeted called party’s voice appears.

Investigator Pro Reporting Highlights

- *CallPlayer Pro™ includes an investigator-friendly screen featuring key information along with the ability to control the playback speed, skip over silent portions of the call and make reporting notes that can be searched at a later date.*
- *VoiceSearch™ finds where an offender’s voice appears on all calls. Authorized users can also search on a called party’s voice and identify the calls on which that called party’s voice appears.*
- *MyCallReview™ lets you find, filter, manage and return to calls you’ve listened to.*
- *NoteManager™ lets you organize, view and report on notes across calls.*
- *ReportMaker™ effortlessly runs reports to uncover patterns of telephone system use that may indicate illicit activities.*
- **Allowed Calling List (ACL) Audit Report** - Report sent monthly to the TDCJ OTS office, summarizing audits performed on Allowed Numbers ensuring they have not ported to unauthorized services or otherwise changed registration information.

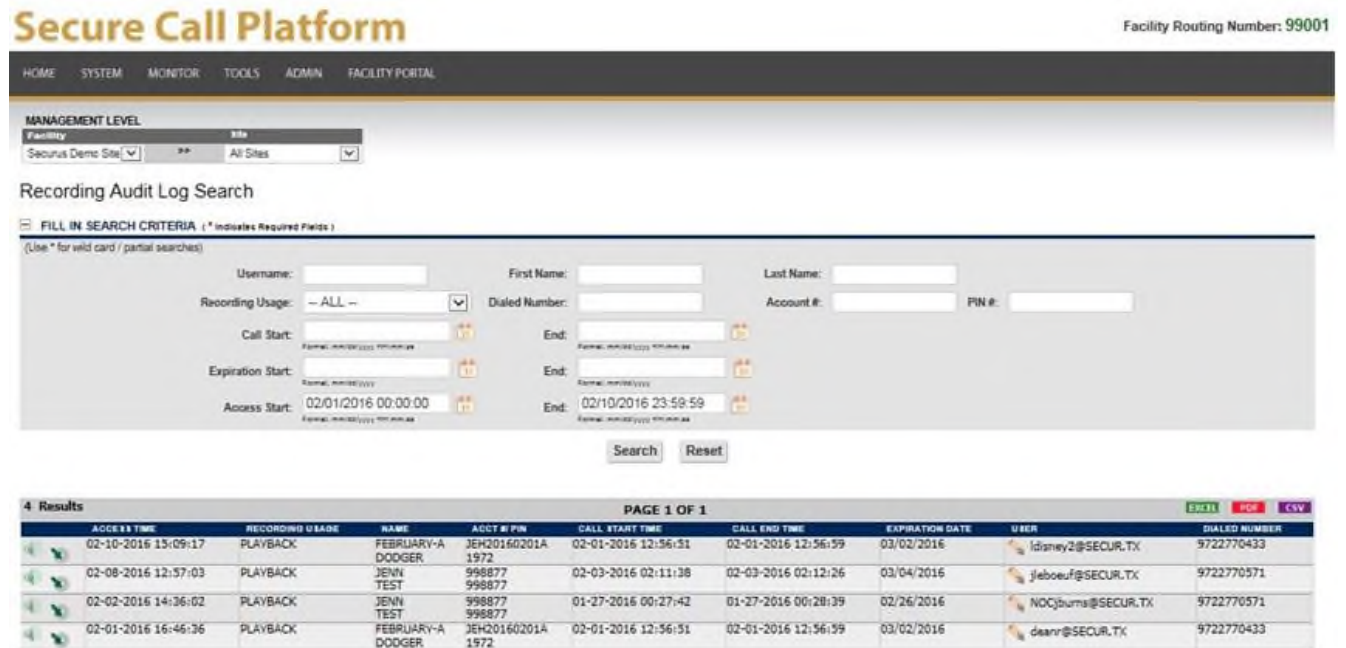
14. **Proposer shall describe in detail the procedures required to monitor Offender conversations, record Offender conversations and terminate Offender calls from any designated Department location. Proposer shall specifically state what equipment will be used to accomplish the monitoring requirement. (C.3.1.1.H)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The OTS has an integrated recording and monitoring system that allows authorized users to access all offender conversations, minus those that are marked as private. Multiple levels of security provide that only authorized personnel can access and monitor the offender recordings. Through the SCP portal, authorized personnel can listen to live or archived recordings via any device connected to the internet.

The CenturyLink Team acknowledges that all recordings and call records are considered evidence and become the exclusive property of the Department. We fully understand the chain of evidence process, and as an added benefit to the Department we will make available records of any activities that have occurred surrounding any live monitored call or recording.

The SCP portal tracks all user activity when accessing any of the applications. When users access recordings, SCP will track whether the recordings were played back, live monitored, copied to a management folder, downloaded or burned to a CD. This information is accessible by authorized Department staff through SCP in a user friendly, easy to use report. This report provides the capability to search by individual user or by specific event, such as all recordings accessed for playback.



Secure Call Platform Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Factory Site
 Securus Demo Site All Sites

Recording Audit Log Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)
 (Use * for wild card / partial searches)

Username: _____ First Name: _____ Last Name: _____
 Recording Usage: -- ALL -- Dialed Number: _____ Account #: _____ PIN #: _____
 Call Start: _____ End: _____
 Expiration Start: _____ End: _____
 Access Start: 02/01/2016 00:00:00 End: 02/10/2016 23:59:59

Search Reset

4 Results PAGE 1 OF 1 [Excel](#) [PDF](#) [CSV](#)

ACCESS TIME	RECORDING USAGE	NAME	ACCT #/ PIN	CALL START TIME	CALL END TIME	EXPIRATION DATE	USER	DIALED NUMBER
02-10-2016 13:09:17	PLAYBACK	FEBRUARY-A DODGER	JEH20160201A 1972	02-01-2016 12:56:51	02-01-2016 12:56:59	03/02/2016	ldaney2@SECUR.TX	9722770433
02-08-2016 12:57:03	PLAYBACK	JENIN TEST	998877 998877	02-03-2016 02:11:38	02-03-2016 02:12:26	03/04/2016	jleboeuf@SECUR.TX	9722770571
02-02-2016 14:36:02	PLAYBACK	JENIN TEST	998877 998877	01-27-2016 00:27:42	01-27-2016 00:28:39	02/26/2016	NOCjburns@SECUR.TX	9722770571
02-01-2016 16:46:36	PLAYBACK	FEBRUARY-A DODGER	JEH20160201A 1972	02-01-2016 12:56:51	02-01-2016 12:56:59	03/02/2016	deann@SECUR.TX	9722770433

This tracking mechanism is also integrated throughout the call detail reports in order to give authorized department staff a quick view to determine if a call had been accessed while running a standard call detail report. This indication of the recording accessed will show up in the form of a “padlock” icon. An additional layer of security provides even higher level authorized staff the ability to click the “padlock” and view the complete call access history details including Access Date, Access Type, User, Dialed Number, and Access Protocol if the session was via Department facility or remote access (http / https).

Secure Call Platform

 Facility Routing Number: **99001**

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL ADMINISTRATION TOOL REVERSE BNA LOOKUP

MANAGEMENT LEVEL

Facility	Site	Phone Group	Phone
Securus Demo Site	All Sites	All Phone Groups	All Phones

Call Detail Records Search









Saved Searches


FILL IN SEARCH CRITERIA (* Indicates Required Fields)

29 Results

PAGE 1 OF 1

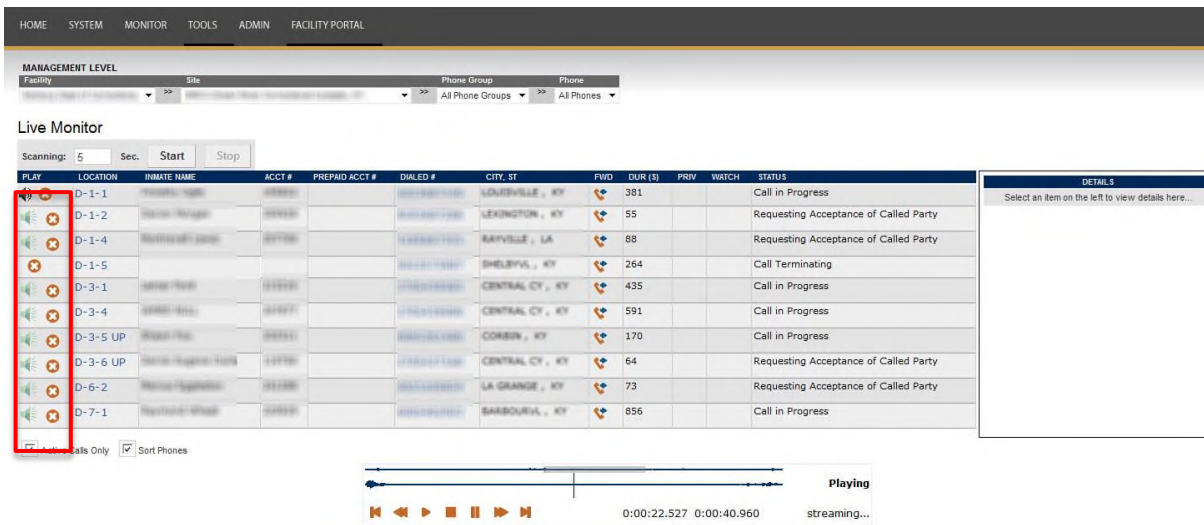
EXCEL PDF CSV

	SITE	PORT LOC	DIALED #	GEO LOC	START	END	DUR	ACCT # PIN	PREPAID ACCT#	NAME	AGENCY TYPE	CALL TYPE	CALL STATUS	TERM CAT	BLOCKED REASON	CALL PROPERTIES
 	Securus Demo Site	LP 1	(1) 3722270648 Local		02-13-2018 11:56:11	02-13-2018 11:56:40	29 (s) 0.48 (m)	77547 777547		CHRISTOPHER DOLLITTLE		Debit	complete	Called party hangup		Language: English Voice Biometrics IPro Pin Check CVV Charge: \$3 Taxes & Fees: \$0.32
 	Securus Demo Site	LP 1	(1) 3722270648 Local		02-13-2018 12:05:03	02-13-2018 12:05:37	34 (s) 0.57 (m)	77547 777547		CHRISTOPHER DOLLITTLE		Debit	complete	Called party hangup		Language: English Voice Biometrics IPro Pin Check CVV Charge: \$3 Taxes & Fees: \$0.32
 	Securus Demo Site	LP 16	(1) 3722270379 Local		02-13-2018 12:06:48	02-13-2018 12:07:11	23 (s) 0.38 (m)	6311 6311		KEN BURNS	FLDOC	Debit	complete	Called party hangup		Language: English Voice Biometrics IPro Pin Check CVV Charge: \$3 Taxes & Fees: \$0.32
 	Securus Demo Site	LP 1	(1) 3722270648 Local		02-13-2018 12:50:12	02-13-2018 12:50:31	19 (s) 0.32 (m)	77547 777547		CHRISTOPHER DOLLITTLE		Debit	complete	Called party hangup		Language: English Voice Biometrics IPro Pin Check CVV Charge: \$3

 Save selected calls to folder

Call Monitoring

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 offender 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, offender 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.”

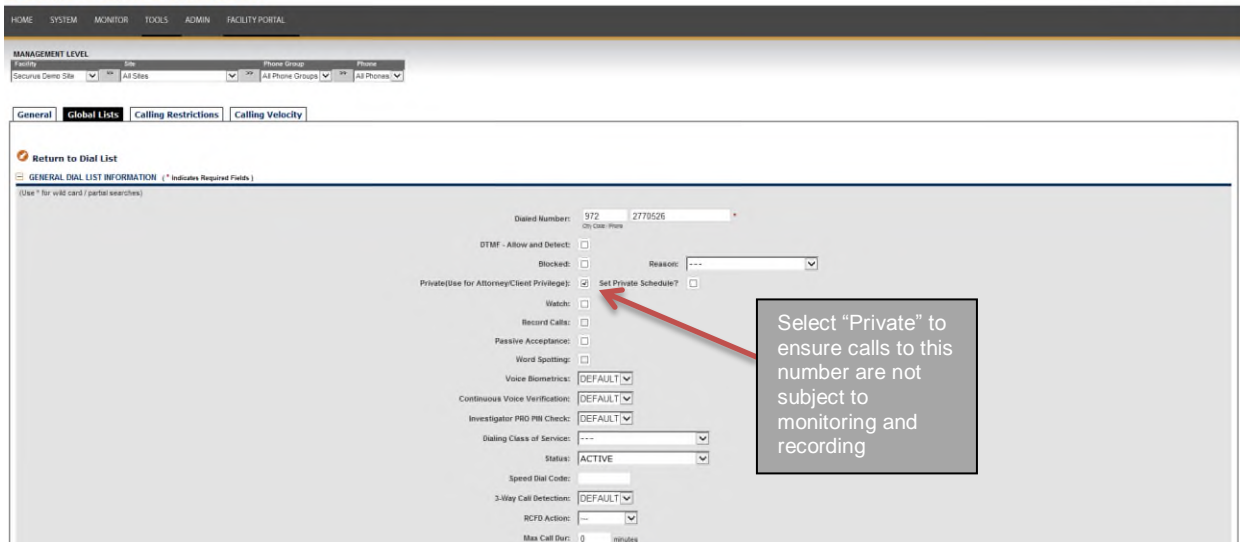


The screenshot shows the SCP Live Monitor interface. At the top, there is a navigation menu with options: HOME, SYSTEM, MONITOR, TOOLS, ADMIN, FACILITY PORTAL. Below this is a 'MANAGEMENT LEVEL' section with dropdown menus for Facility, Site, Phone Group, and Phone. The main area is titled 'Live Monitor' and includes a 'Scanning' section with a value of 5, and 'Start' and 'Stop' buttons. A table lists active calls with columns: PLAY, LOCATION, INMATE NAME, ACCT #, PREPAID ACCT #, DIALED #, CITY, ST, FWD, DUR (\$), PRIV, WATCH, STATUS. A red box highlights the 'PLAY' column icons. Below the table is a 'Details' panel with a 'DETAILS' header and a message: 'Select an item on the left to view details here...'. At the bottom, there is a playback control bar with a progress slider, play/pause buttons, and a 'Playing' indicator.

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.

Secure Call Platform

Facility Routing Number: 99001



The screenshot shows the 'Secure Call Platform' configuration interface. At the top, there is a navigation menu with options: HOME, SYSTEM, MONITOR, TOOLS, ADMIN, FACILITY PORTAL. Below this is a 'MANAGEMENT LEVEL' section with dropdown menus for Facility, Site, Phone Group, and Phone. The main area is titled 'Global Lists' and includes a 'Return to Dial List' button. A section titled 'GENERAL DIAL LIST INFORMATION (* Indicates Required Fields)' contains various configuration options for a dial list. A red arrow points to the 'Set Private Schedule?' checkbox, which is checked. A text box next to the arrow contains the text: 'Select "Private" to ensure calls to this number are not subject to monitoring and recording'. Other options include 'DTMF - Allow and Detect', 'Blocked', 'PrivateUse for Attorney/Client Privilege', 'Watch', 'Record Calls', 'Passive Acceptance', 'Word Spotting', 'Voice Biometrics', 'Continuous Voice Verification', 'Investigator PIV Check', 'Dialing Class of Service', 'Status', 'Speed Dial Code', '3-Way Call Detection', 'BCFD Action', and 'Max Call Dur'.

Call Monitoring, Silent

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

Covert Alert

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

Covert Alert bridges a call to an authorized remote number for dialed numbers, phones, or offender PINs that 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 offender, 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.

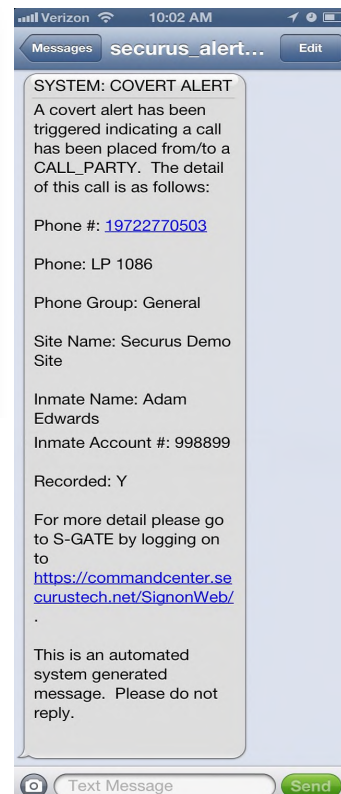
Covert Alert can send calls to any phone number within the facility or across the United States. Investigators can also monitor calls through on-site workstations using the SCP Live Monitor, or remote live call-forwarding feature. This allows facility investigators to monitor potential illicit activities 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, offender 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, offender PIN, originating telephone, dialed number, and an indication if the call has been recorded.



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 offender at the TDCJ facility. To accept this Covert Alert call, please enter your investigator PIN now.”

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.

SCP writes all recorded calls to a Network Attached Storage array (NAS) in our primary Data Center. Each NAS array is also replicated to the secondary Data Center for redundancy and failover. All recordings created on the platform reside in at least two of our Data Centers. Recordings are stored on-line for immediate access for the contractually agreed upon time. 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.

Recording Search and Retrieval

SCP provides authorized personnel and investigators single-point access to research TDCJ call records and recordings.

Users can specify search criteria, such as called party, calling telephone, date, time, PIN, custody account number, duration, and location, and 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.

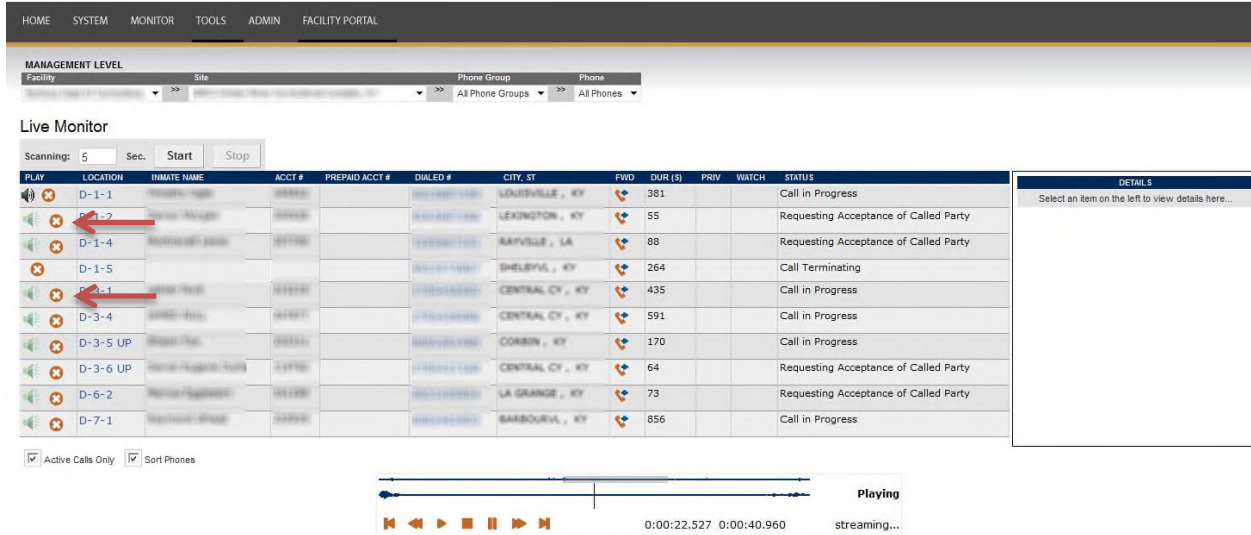
Search results provide detailed information about each call and will indicate whether or not the call detail record (CDR) has an attached recording. If recorded, authorized investigators can listen to the recording using the embedded call player with easy-to-use search capabilities, and features such 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. While it is possible to make a recording from the speakers, this is only a copy of the original. 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 Termination

Authorized personnel can terminate a call in progress from the “live monitoring” page by clicking on the red X.



The screenshot displays the 'Live Monitor' interface. At the top, there are navigation tabs: HOME, SYSTEM, MONITOR, TOOLS, ADMIN, and FACILITY PORTAL. Below this is a 'MANAGEMENT LEVEL' section with dropdown menus for Facility, Site, Phone Group, and Phone. The main area is titled 'Live Monitor' and includes a 'Scanning: 5 Sec.' control with 'Start' and 'Stop' buttons. A table lists active calls with the following columns: PLAY, LOCATION, INMATE NAME, ACCT#, PREPAID ACCT#, DIALED #, CITY, ST, FWD, DUR (S), PRIV, WATCH, STATUS, and DETAILS. The table contains 12 rows of call data. A red 'X' icon is present in the 'PLAY' column for rows 2, 3, 4, and 5. Below the table are checkboxes for 'Active Calls Only' and 'Sort Phones'. At the bottom, there is a playback control bar with a progress bar, a 'Playing' indicator, and a 'streaming...' status.

Additionally, Cover Alert includes a “Barge In” feature which allows the investigator to 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 offender 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.

15. **Proposer shall provide a full description of the Digital Recording System (DRS), to include the indication function of recording space remaining and mirrored storage capability. (Section C.3.1.1.J)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The OTS includes a full-time digital recording system that covers all TDCJ OTS telephone lines with additional growth capacity to allow for expansion of the OTS.

Our OTS centralized solution provides an advanced method of aggregating data and providing centralized recording of a large system with many remote satellite facilities. Each remote site is connected to a central site that provides centralized management of resources allowing on-the-fly growth of telephone facilities and recording storage.

Recording Search and Retrieval

Call recordings are available for playback immediately. The OTS can simultaneously record all telephone circuits while providing audio outputs for listening to selected calls from facility, regional, and administrative locations. Multiple users listening to a single recorded conversation will not affect the operation or quality of the recorded conversation of the OTS. All calls are

recorded in their entirety with exception of confidential attorney-client communication. Playback from any drive or other recording media will not interrupt the recording process.

The OTS includes a “library” that catalogs and indexes every call transmission allowing for fast retrieval of recording. Users can search and retrieve recordings by specifying search criteria, such as called party, calling telephone, date, time, PIN, custody account number, duration, and location, and search across a site or group of sites based on their security authorization. The system will automatically make time and date or daylight savings time adjustments for the recording.

Search results provide detailed information about each call and will indicate whether or not the call detail record (CDR) has an attached recording. If recorded, authorized investigators can listen to the recording using the embedded call player with easy-to-use search capabilities, and features such as, pause and play.

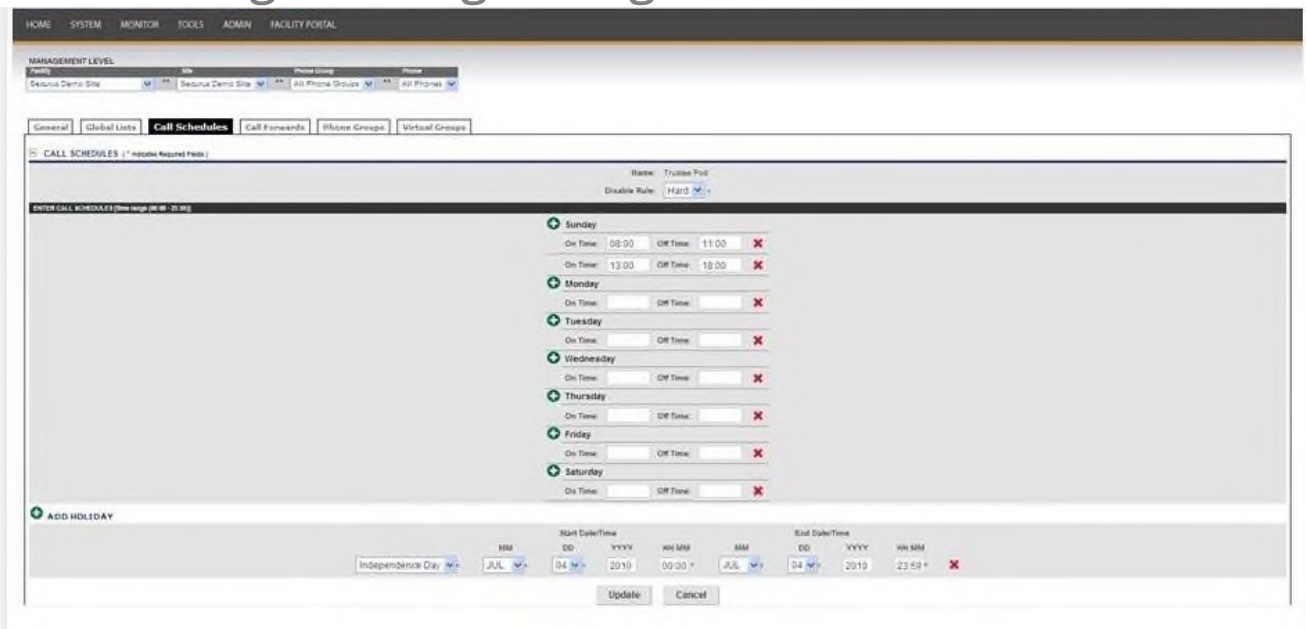
To speed searching of a recording the player shows sound wave activity of the call to identify times of limited talk or to identify a particular event.

SCP streams call recordings to a program on an investigator’s computer that can ‘play’ the recording through the attached speakers.

Establishing Recording Schedules

As all calls are recorded, except those marked as private, the method of controlling recording schedules through our OTS system is by controlling the calling schedules. Calling schedules are flexible and configurable allowing the facility to have multiple on and off times during the day, within a week and by day of the week and then be applied to individual telephones, groups of telephones, individual offenders and/or globally.

Programming Calling Schedules



Call Recording Storage

The call recordings will be stored for 36 months for on-line retrieval of local and remote locations on multiple Network Attached Storage array (NAS). Each NAS array is also replicated to the secondary Data Center for redundancy and failover. The need to back-up data is not required since the recorded conversations are replicated to a separate network during creation.

The OTS 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.

The 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. Premises-based systems needed manual backup schemes that are no longer necessary with SCP. SCP writes all recorded calls to a Network Attached Storage array (NAS) in our primary Data Center. Each NAS array is also replicated to the secondary Data Center for redundancy and failover. All recordings created on the platform reside in at least two of our Data Centers.

The NAS architecture makes all storage available to all servers on the network. The NAS solution delivers complete scalability for a facility's storage requirements and supports data migration from one storage device to another and the sharing of data among different servers in a network. The NAS devices provided by EMC can scale simply by adding another node of dense SATA disk to the storage array. Within the NAS, SCP uses a software defined storage platform of very dense disk nodes. Even if three individual hard disk drives fail or one node fails, during the disk or node recovery process, the system will continue to operate without data loss.

The Securus NAS has more than 7 petabytes of storage space in each carrier-class data center 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 NOC monitors call traffic patterns, bandwidth detail, and network life cycle management to ensure sufficient resources are in place. A separate capacity engineering team reviews storage requirements and traffic volume reports throughout all systems. Since SCP records all calls, except those marked as private, the OTS establishes and controls schedules to initiate and suspend recording by controlling calling schedules. SCP has automated calling schedules which allows the system to manage the scheduling policies of the facility without staff intervention. Calling schedules are used to turn on and off the phones during designated times throughout the day or night.

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

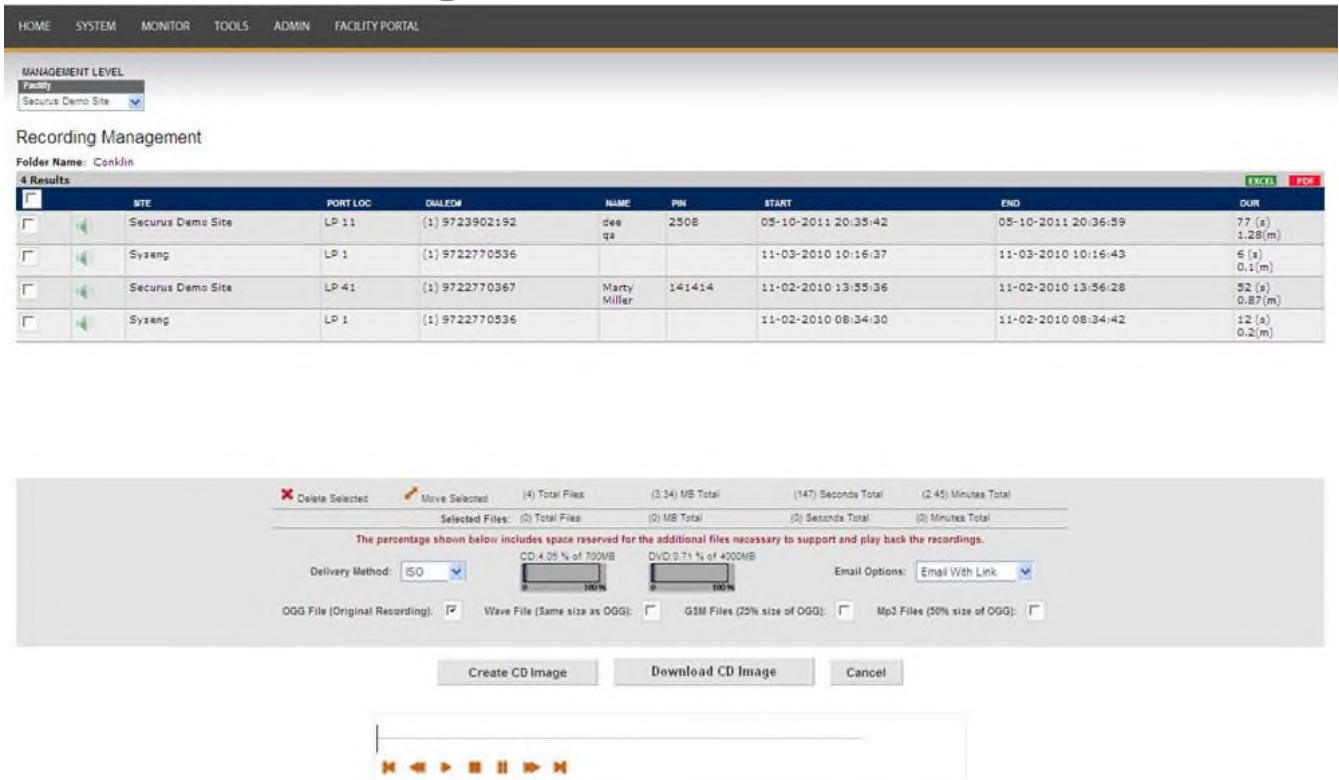
- **Scalable** to meet any facility's contractually required storage demands
- **Resistant** to local disasters through multiple copies stored within the data centers and off-site
- **Highly available** through the unique architecture and design of the data storage model
- **Partitioned** and **compressed** 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 within both carrier-class data centers. Typically, call detail records are stored for the life of the contract and retained per contractual obligation.

Downloading Recordings

SCP allows authorized users to copy recorded conversations to any external media device connected to the user's PC, such as CD, DVD, mp3 player, or USB drive. This feature facilitates easy sharing of recordings for investigative or court purposes. To maintain the accuracy of data and recordings during downloading and copying, SCP stores the files—both audio and CDR information—embedded within an industry-standard read-only format that prevents the possibility of tampering.

Downloading Calls to External Media



The screenshot displays the SCP Recording Management interface. At the top, there is a navigation menu with options: HOME, SYSTEM, MONITOR, TOOLS, ADMIN, FACILITY PORTAL. Below this, the 'MANAGEMENT LEVEL' is set to 'Facility' and the selected facility is 'Securus Demo Site'. The main section is titled 'Recording Management' and shows 'Folder Name: Conklin' with '4 Results'.

SELECT	SITE	PORT LOC	NUMBER	NAME	PIN	START	END	DIR
<input type="checkbox"/>	Securus Demo Site	LP 11	(1) 9723902192	dee qa	2508	05-10-2011 20:35:42	05-10-2011 20:36:59	77 (s) 1:28(m)
<input type="checkbox"/>	Syaeng	LP 1	(1) 9722770536			11-03-2010 10:16:37	11-03-2010 10:16:43	6 (s) 0:1(m)
<input type="checkbox"/>	Securus Demo Site	LP 41	(1) 9722770367	Marty Miller	141414	11-02-2010 13:55:36	11-02-2010 13:56:28	52 (s) 0:57(m)
<input type="checkbox"/>	Syaeng	LP 1	(1) 9722770536			11-02-2010 08:34:30	11-02-2010 08:34:42	12 (s) 0:2(m)

Below the table is a download options dialog box. It shows 'Delete Selected' and 'Move Selected' options. Summary statistics include: (4) Total Files, (3.34) MB Total, (147) Seconds Total, (2:45) Minutes Total. Selected files summary shows (0) Total Files, (0) MB Total, (0) Seconds Total, (0) Minutes Total. A warning states: 'The percentage shown below includes space reserved for the additional files necessary to support and play back the recordings.' Delivery Method is set to ISO. Progress bars show CD at 4.05% of 700MB and DVD at 0.71% of 4000MB. Email Options are set to 'Email With Link'. File format options include OGG File (Original Recording) [checked], Wave File (Same size as OGG) [unchecked], GSM Files (25% size of OGG) [unchecked], and Mp3 Files (50% size of OGG) [unchecked]. Buttons for 'Create CD Image', 'Download CD Image', and 'Cancel' are visible.

When downloading calls, the user creates a folder within SCP to save the calls, and the interface identifies the remaining space available.

16. **Proposer shall describe how the Uninterrupted Power Supply (UPS) functions during power outages, surges and spikes, as well as identify exactly what equipment will be equipped with UPS protection. Proposer shall provide specific details on the recording systems, back-up and restore procedures, as well as identification of site locations where data ups will be stored and backed-up. (Section 3.1.1.K)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The CenturyLink Team provides Uninterrupted Power Supply (UPS) at both the facility level as well as at the Securus data center as a redundant back up to ensure that in the event of loss of power, there is no change in the operational characteristics of the system. Additionally, we proactively monitor the OTS and have established a redundant system to ensure maximum facility uptime.

Uninterruptible Power Supply Facility Backup

SCP is a fully self-contained system, requiring minimal AC power dedicated to on-site equipment. That being said, each Department facility will continue to have an uninterruptible power supply (UPS) backup for the equipment installed on the premises. The UPS eliminates spikes, sags, surges, transients, and all other over/under voltage and frequency conditions, providing clean power to connected critical loads.

Powerware



We use the PowerWare UPS, which is only 7.6 inches high x 5.9 inches wide x 15.4 inches deep, minimizing the space required in the facility equipment room. This rack mount UPS is a high-density backup power protection solution that is ideal for servers, storage systems, network equipment and other critical devices. The UPS is self-charged, and the equipment self-initializes without manual intervention when commercial power is restored.

Calls In Progress

The Integrated Access Device (IAD) and uninterruptible power supply (UPS) maintain all in-progress telephone calls for up to 30 minutes, while blocking additional call attempts after the event. After 30 minutes, the system terminates all calls in progress and powers down to a quiescent state that allows it to resume full operation automatically after the restoration of commercial power.

When commercial power is lost, there is no change in the operational characteristics of the system. If commercial power is not restored prior to exhausting UPS power, the system terminates all calls in progress and shuts down. The system will fully recover from any power failure automatically, within five (5) minutes, with no outside intervention required after power is restored. When commercial power is restored prior to the exhaustion of UPS power, no change in the operational characteristics of the system will occur.

Uninterruptible Power Supply Data Center Backup

Securus operates and maintains two major data centers networked to the equipment installed on TDCJ premises. Each data center has an uninterruptible power supply (UPS), and a generator to provide maximum network uptime. The traditional data circuits (MPLS, Frame Relay, VoIP) all have dual connectivity feeds to/from the telecommunication carrier to each of our data centers.

The UPS systems in our primary data center have 2N redundancy. Dual source power runs through a static bypass switch. Battery rooms support the UPS systems with gel cell battery banks. Fifteen minutes of battery backup is available at full load (such as 90 watts per square foot). Each battery bank is continuously monitored to ensure optimal operation. Upon loss of commercial power for more than 15 seconds, paralleling switchgear automatically powers all nine generators; generators are shed to cover load as needed. Typically, the transition from UPS to generator power takes 60 seconds.

Data Center Power Conditioning

The uninterruptible power supply (UPS) system filters, spikes, sags, surges, transients, and all other over/under voltage and frequency conditions, providing clean power to connected critical loads. Power distribution units (PDUs) distribute power to individual customer racks via remote power panels. Each rack has redundant power strips (A & B) routed to diverse PDUs. Diverse uninterruptible power supply systems feed each power distribution unit.

Diesel Generator(s)

There are multiple diesel generators providing standby power to the Internet Data Center. At 90-watts per sq. ft., this represents a N+2 configuration. Five (5) underground fuel tanks store 70,000 gallons of diesel on-site.

Cooling

The building has five (5) 600-ton chillers. The raised floor, which is used as an air plenum, delivers conditioned air to the equipment cabinets/racks. Multiple 29 - ton CRAC units are strategically located on the raised floor area. CRAC units deliver conditioned air at 55° F to maintain a room temperature of 72° F. If a chiller fails, a standby chiller will carry the load. The standby chiller is designed to operate continuously. The system is fully redundant, designed to N+1 requirements.

UPS

There are six (6) Liebert UPS systems, each with four (4) - 600kW/750kVA modules. Power is supplied to the UPS systems through commercial power feeders and standby generators.

HVAC

Designed to N+1 specification, Computer Room Air Conditioning (CRAC) units deliver conditioned air at 55° F to maintain a room temperature of 72°F. The building maintenance group performs 24x365 monitoring. Onsite personnel respond to alarms per Securus standards. Local alarms are also remotely monitored in the Local Exchange Carrier (LEC) Global Client Service Center (GCSC) in Alpharetta, GA. Humidity levels are monitored by the CRAC units at the point of air intake and by additional sensors located throughout the data center. Pre-set threshold levels are monitored by the infrastructure monitoring systems.

Water Detection

Water and humidity are closely monitored in the sub-floor air plenum by highly sensitive moisture sensing devices.

Fire Suppression

Both the proposed LEC Global Internet Data Centers (GIDCs) feature pre-action dry pipe fire suppression systems supported by state-of-the art VESDA smoke detection and alarm systems. The VESDA system is considered 100 times more sensitive than conventional, passive fire detection systems. Conventional smoke detectors are also utilized and are grouped into zones. When one or more detectors in different zones detect smoke, the fire alarm panel opens the deluge valve to fill the sprinkler piping with water. In case of an actual fire, the seal on the sprinkler heads will melt and discharge water on the affected area. Water will not be discharged in unaffected areas. Fire extinguishers are located throughout the Data Center floor to accommodate human intervention.

The system is designed to avoid accidental water damage due to leaks in the pipes. The system contains pressurized gas and is monitored against a reduction in that pressure which would indicate a leak in one of the pipes.

The fire detection system has several steps to prevent false alarms. The VESDA (Very Early Smoke Detection and Alarm) system provides the first indication that there might be a fire. Then a smoke detector must detect smoke. Then a second smoke detector must independently detect smoke. Follow this third level of detection; the dry-pipes will fill with water.

The system is designed to apply water only to the areas where there is a fire. The only way for a sprinkler to activate is for the temperature at that sprinkler to exceed 170 degrees F. At which point the head melts and releases water. It has been found that 3 sprinklers (or less) are usually sufficient to suppress the majority of all fires. Water is not released generally throughout the data center.

In the event of a fire and release of water to suppress the fire, any equipment that is sprayed would most probably short to ground. Each rack is protected by 20-Amp circuit breakers. The short would cause too much power to be drawn and the circuit would be tripped shutting off power to individual racks and not to the entire center.

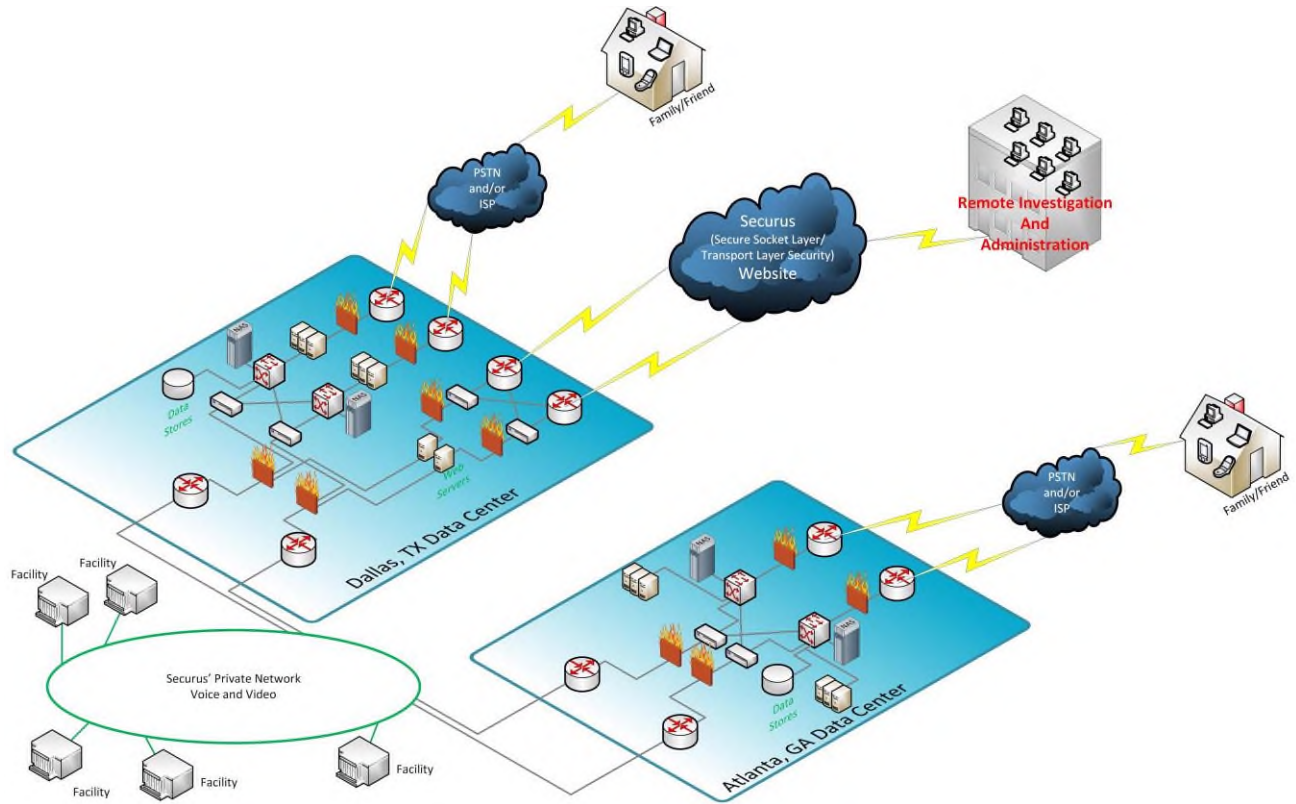
Recording Systems: Back-Up and Restore Procedures

Call Recording Storage

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.

SCP writes all recorded calls to a Network Attached Storage array (NAS) in our primary Data Center. Each NAS array is also replicated to the secondary Data Center for redundancy and failover. All recordings created on the platform reside in at least two of our Data Centers.

The NAS architecture makes all storage available to all servers on the network. The NAS solution delivers complete scalability for a facility's storage requirements and supports data migration from one storage device to another and the sharing of data among different servers in a network. The NAS devices provided by EMC can scale simply by adding another node of dense SATA disk to the storage array. Within the NAS, SCP uses a software defined storage platform of very dense disk nodes. Even if three individual hard disk drives fail or one node fails, during the disk or node recovery process, the system will continue to operate without data loss.



The Securus NAS has 7 petabytes of storage space in each carrier-class data center 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

Restore Procedures

Securus Technologies has designed and implemented a robust network architecture that provides for quick disaster recovery, minimalizing downtime for the OTS platform and its customers.

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 two data centers in two 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.

Tier 1 – Basic Small Business <ul style="list-style-type: none"> • 99.671% availability • Susceptible to disruptions • Single path for power • No redundant components 	Tier 2 – Redundant Medium Business <ul style="list-style-type: none"> • 99.741% availability • Less susceptible to disruptions • Single path for power • Redundant components
Tier 3 Large Business <ul style="list-style-type: none"> • 99.982% Availability • Planned activity without disruption • Multiple paths for power • Redundant components 	Tier 4 Multi-Million \$ Business <ul style="list-style-type: none"> • 99.95% Availability • Can withstand at least one worst-case event • Multiple paths for power • Redundant components

TIA-942 Infrastructure standards for data centers
Telecommunications Industry Association

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.

Redundancy

Redundancy is a key component of the Secure Call Platform (SCP). While operating on a single platform, 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 offender 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 define 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 carry 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 Offender Telephone Systems (OTS) 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.

SolarWinds® Typical Monitored Application Elements

Application Details

MANAGEMENT: [Edit Application Monitor](#) Unmanage
[Poll Now](#)

[Real-Time Process Explorer](#)
[Service Control Manager](#)
[Real-Time Event Log Viewer](#)

APPLICATION NAME: **Windows Server 2003-2008 (RPC)** on ...

APPLICATION STATUS: ● Application status is Up

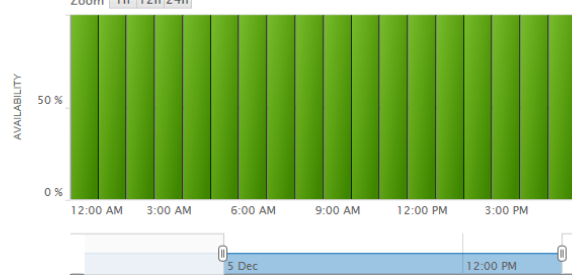
SERVER STATUS: ● Server status is Up

COMPONENT NAME	COMPONENT TYPE	COMPONENT STATUS
● Distributed Transaction Coordinator	Windows Service Monitor	Up
● Network Connections	Windows Service Monitor	Up
● Number of Processes	WMI Monitor	Up
● DHCP Service Monitor	Windows Service Monitor	Up
● Total Available Memory (MBytes)	Performance Counter Monitor	Up
● Page File Usage	Performance Counter Monitor	Up
● Disk Queue Length	Performance Counter Monitor	Up
● Number of Threads	Performance Counter Monitor	Up
● File read bytes per second	Performance Counter Monitor	Up
● File write bytes per second	Performance Counter Monitor	Up
● Remote Registry Service	Windows Service Monitor	Up

Application Availability

Windows Server 2003-2008 (RPC)
 Dec 5 2017, 12:00 am - Dec 5 2017, 5:00 pm

Zoom:



AVAILABILITY: 50%
0%

12:00 AM 3:00 AM 6:00 AM 9:00 AM 12:00 PM 3:00 PM

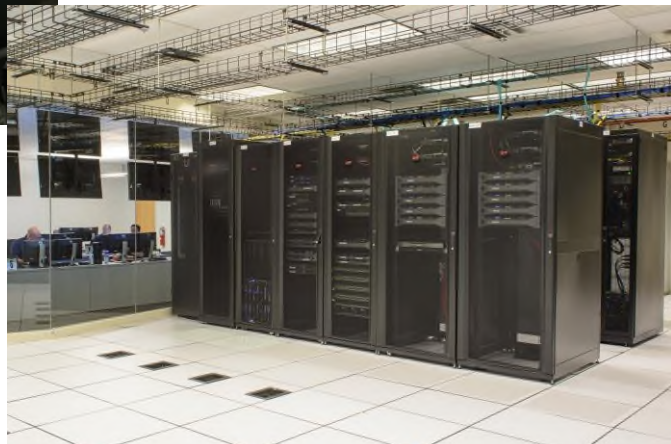
5 Dec 12:00 PM

Legend: ■ Other, ■ Up, ■ Critical, ■ Unknown, ■ Warning, ■ Down

Processes and Services

COMPONENT NAME	PROCESS NAME (ID)	CPU LOAD	MEMORY USED			IOPS
			PHYSICAL	VIRTUAL		
● DHCP Service Monitor	DHCP (792)	0	0.25	0.11		19.89 / Sec
● Distributed Transaction Coordinator	MSDTC (17380)	0	0.08	0.01		0.00 / Sec
● Network Connections	Netman (1196)	0	0.12	0.02		0.00 / Sec

Securus Primary Network Operations Center



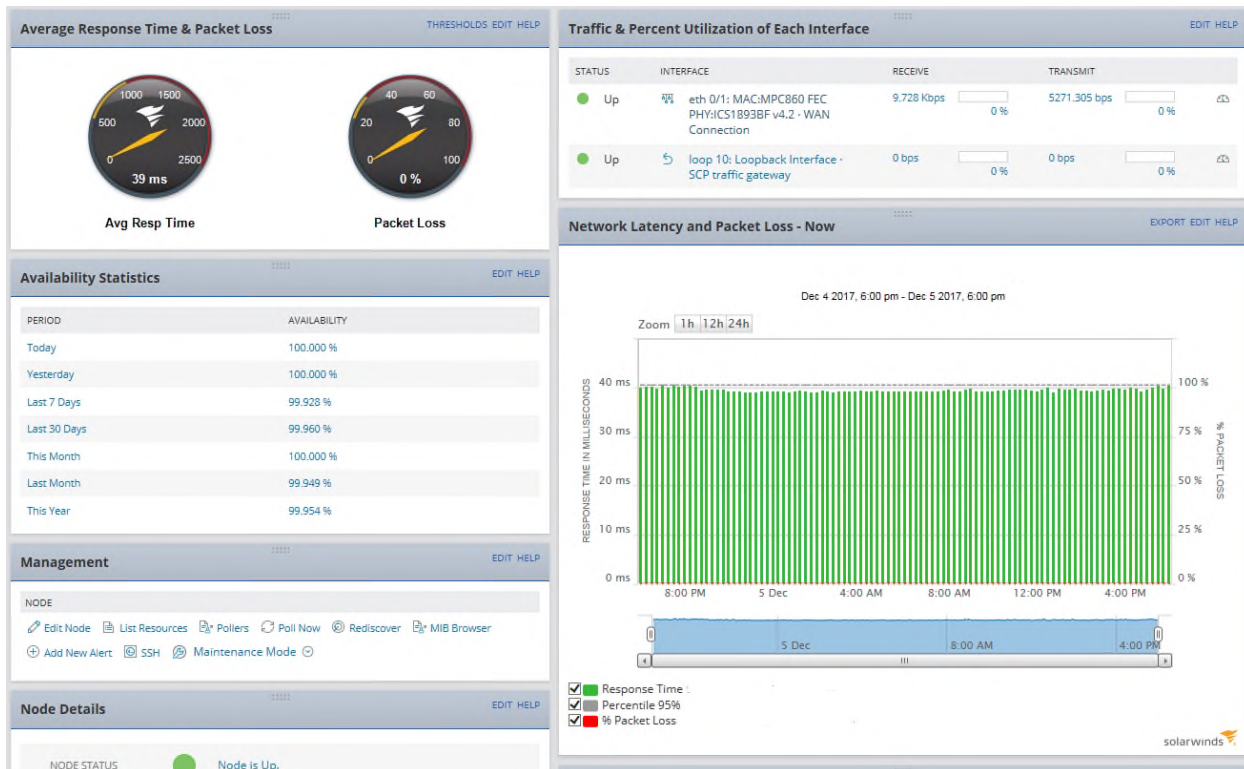
Premise Equipment

The Securus Technical Support team provides 24x7x365 monitoring of all facility-based equipment and directly supports facility installations via telephone and email. Technical Support monitors connectivity for all installations and all installed equipment including Integrated Access Devices (IADs), Visitation Phone Monitoring (VPM) units, switches and Uninterrupted Power Supply (UPS) systems. The systems are polled every two minutes and their vital operating statistics are sent every 10 minutes. Upon receiving an alert indicating network failure, Securus will open a trouble ticket with the appropriate circuit provider. In the case of a premise-based equipment failure, a Field Technician is dispatched to the facility for on-site repair.

A technician visits every TDCJ site at least once a month to inspect premise equipment.

Additionally, we perform preventative maintenance on all equipment 1x a quarter.

SolarWinds® Device Monitoring Example



Bandwidth & Network Latency Monitoring Example

In addition to real-time monitoring and alerting, Securus Technical Support also leverages the SolarWinds® network performance monitor to gather and evaluate historical data for network alerts, bandwidth usage, packet loss, and hardware performance. The detailed level of monitoring available via our network performance monitor allows the Technical Support group to take proactive steps to prevent or mitigate facility outages and to ensure the correct resources are engaged if dispatch is necessary.

Restoration

Platform and Network

In the event of a disaster impacting SCP or our network, Securus immediately assembles a team of engineers to begin investigation and restoration of services. Securus maintains a schedule of on-call personnel for immediate response to service-impacting events and will also engage 3rd party vendors if required.

Facility-installed Systems

We prioritize recovery of premise-based equipment by facility type and equipment location. Maximum-security institutions and institutions with high offender phone usage receive priority. Prioritization also considers customer requirements and preferences. Securus has developed procedures (checklists) to protect personnel and equipment in the event of an emergency situation. Securus will combine headquarters and field staff efforts to expedite service recovery wherever possible. Securus coordinates each checklist to ensure compliance with each facility's guidelines.

Securus has a field support department with more than 224 field service associates supported by a centralized field dispatch team. The Field Service Technicians (FST) are strategically located to support ongoing maintenance as well as any disaster recovery situations. The FSTs are supported by senior technical support resources and engineering to expedite repairs and minimize customer downtime.

Reporting

Upon confirmation of a service impacting event, the Network Operations Center will issue an internal Service Interruption Report (SIR). The SIR will include the nature of the outage, impact to facilities and estimated time of restoration if known. Each incident is assigned an urgency level based on the level of customer impact.

Customer contact personnel receive SIRs, so they can communicate with customer facilities proactively or reactively as required by the facility. Additionally, when possible, Technical Support may communicate a service impacting event via a splash screen in the SCP user interface, the customer interface to SCP. Regular updates ensure that information provided is always current. Securus executives also receive all SIRs, so they are aware of all customer-impacting events.

The NOC will issue a final SIR upon issue resolution. Securus investigates each incident and completes a root-cause analysis (RCA) following all service impacting events. Once the root cause is determined, Securus makes RCA documents available customers upon request.

- 17. Proposer shall describe the Announcements and Call Branding system, and how acceptance will function with both touchtone and rotary dial telephones. (Section C.3.1.1.L)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The 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 and announcements to establish call acceptance and to assist inmates and called parties throughout the calling process. The announcements and call branding

system are all configurable. We have already customized these for your facilities, including Spanish prompts, saving time in implementation.

The inmate calling process is:

1. The inmate picks up the telephone.
2. The inmate hears “For English, press 1.” [In Spanish] For Spanish, press 2.” (Securus can add additional languages on request)
3. “For a collect call, press 1.”
4. “For a debit call, press 2.”

The following table provides calling options and the associated announcements:

Offender Calling Options

Offender Chooses Collect Call Option

Offender Chooses Debit Call Option

“Please enter your TDCJ ID number now”
(repeated)

“Please enter the area code and phone number you are calling now” (repeated)

“You will be asked to verify your name now. Please say your full name after the beep.”

“Thank you, I recognized your voice”

”Please say Texas department of Criminal Justice after the beep.”

“Thank you, I recognized your voice.”

“This call is being recorded and is subject to monitoring. Also note, this call may take a little longer to complete as your called party might be listening to a way in which to put money in your offender debit account by calling (866) 963-7912, (866) 963-7912. You may hear silence during the acceptance of your call. Please continue to hold.”

[call is answered] ”Thank you for using CenturyLink, You may start the conversation now.”

“Please enter your TDCJ ID number now”
(repeated)

“You have (X) dollars and (X) cents.”

“Please enter the area code and telephone number you are calling now.” (repeated)

“This call will cost (X) dollars and (X) cents for the first minute and (X) dollars and (X) cents for each additional minute, plus any applicable telecom and sales taxes.”

“You will be asked to verify your name now. Please say your full name after the beep.”

“Thank you, I recognized your voice”

”Please say Texas department of Criminal Justice after the beep.”

“Thank you, I recognized your voice.”

“This call is being recorded and is subject to monitoring. Also note, this call may take a little longer to complete as your called party might be listening to a way in which to put money in your offender debit account by calling (866) 963-7912, (866) 963-7912. You may hear silence during the acceptance of your call. Please continue to hold.”

[call is answered] ”Thank you for using CenturyLink, You may start the conversation now.”

Specific Friends and Family Process

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

Friends and Family Receiving Call Process

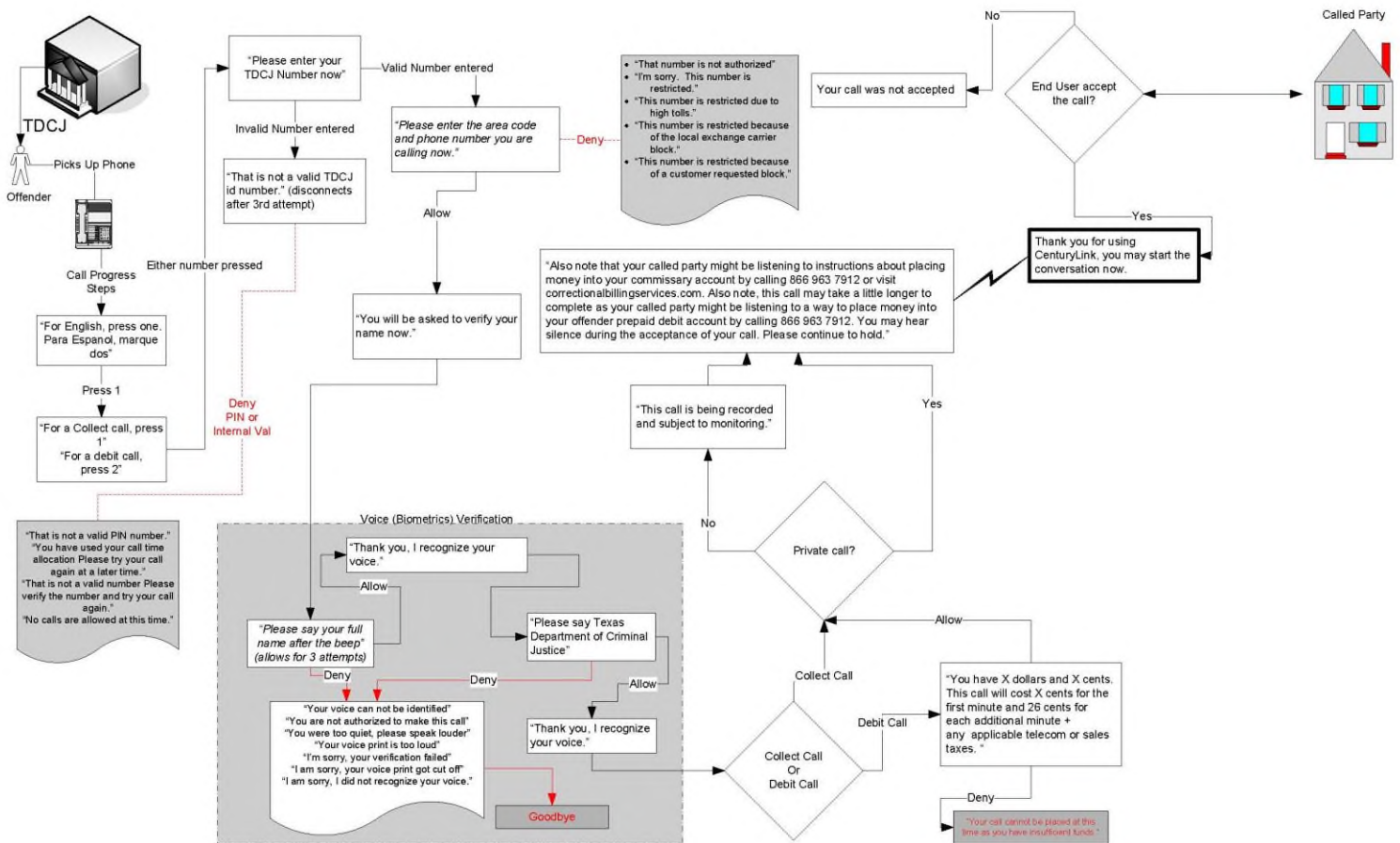
Collect Call	Debit Call
“Hello, This is a collect call from (Offenders Name) an offender at (Unit Name) This call is being recorded and subject to monitoring”	“Hello, This is a free call from (Offenders Name) an offender at (Unit Name) This call is being recorded and subject to monitoring,
“To accept charges, press 1.” “To refuse charges, press 2.” “To learn how to put money in your pre-paid account or an offender pre-paid debit account, press 5.” “If you would like to permanently block your number from receiving calls from this facility, press 6.” “For available credit and rate quote, press 7” [Presses 1] “You may start your conversation now.”	“To accept this free call, press 1” “To refuse this free call, press 2.” “To learn how to put money in your pre-paid account or an offender pre-paid debit account, press 5.” “If you would like to permanently block your number from receiving calls from this facility, press 6.” “For available credit and rate quote, press 7” [Presses 1] “You may start your conversation now.”

In addition to the voice prompts at the initiation of the call, at one minute before the maximum call duration, the “One Minute Remaining” message is played.

Called Party Acceptance

The Secure Call Platform (SCP) requires active “called party” acceptance using touch-tones to complete calls. When the called party answers the phone, the SCP answer detection triggers the call acceptance voice message. This message announces the inmate’s call and asks the called party to accept or reject the charges of a collect call. The called party is instructed to dial a single digit on their telephone to accept the collect call charges, or hang-up to disconnect the call and refuse charges. For rotary phones, the called party can say their selection using voice acceptance.

Inmate Call Flow Chart



18. Proposer shall describe call detail records formats and method to obtain such data, e.g. electronic format via web site. (Section C.3.1.1.M)

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The OTS will provide full call detail records to the Department. The original call detail records are stored in secured databases with access limited to Department approved database administrators only. These databases are also protected through firewalls and the corporate network and cannot be accessed outside of SCP. Additionally, these call records are replicated to several databases for internal operations to use and for SCP to access the records upon request from an authorized system user.

SCP creates a 128 bit encrypted Secure Socket Layer (SSL) connection between the workstation and OTS centralized platform. This connection is established prior to the movement of any data across the network that is confidential or related in any way to the recordings or CDR data. This complex encryption method prevents access or the potential intercept of this data and allows the communication access across the public network to be safe and secure.

The Call Detail Report (CDR) provides an intuitive and user-friendly report to view or search virtually anything related to an offender 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
- 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
- Desired results per page

Please see the following page for a sample Call Detail Report.

Call Detail Report

SECURUS Technologies dinar@SECUR.TX | Help | Log Out

Secure Call Platform Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL ADMINISTRATION TOOL REVERSE BNA LOOKUP

MANAGEMENT LEVEL

Family: Securus Demo Site | Site: All Sites | Phone Group: All Phone Groups | Phone: All Phones

Call Detail Records Search Saved Searches

FILL IN SEARCH CRITERIA (* indicates Required Fields)

(Use * for wild card / partial searches, and text areas with bold label allow multi-entries in comma separated.)

Country Code: [] Dialed Number: [] Destination Zone: -- ALL --

Custody Account #: [] PIN #: [] Prepaid Account #: []

First Name: [] Last Name: [] Agency Type: -- ALL --

Termination Category: -- ALL -- Blocked Reason: -- ALL --

Call Type: -- ALL -- Call Status: Complete

Text2Connect: -- ALL --

Search Notes: []

Tracker #: [] Call Tracker Notes: [] Note Type: -- ALL --

Alternate ID: [] [Add New](#)

Inmate Grouping: [] [Add New](#)

Date Criteria: Date/Time Range | Results Per Page: 100

Start: 04/09/2018 10:11:00 | End: 04/09/2018 12:55:59

[Search](#) [Save Criteria](#) [EXCEL](#) [PDF](#) [CSV](#) [Reset](#)

4 Results PAGE 1 OF 1

ITE	PORT/LOC	DIALED #	REQ LOC	START	END	CHG	ACTY # / PIN	PREPAID ACCT#	NAME	AGENCY TYPE	CALL TYPE	CALL STATUS	TERM CAT	BLOCKED REASON	CALL PROPERTIES
Securus Demo Site	iPhone	(1) 2127231327 Local		04-09-2018 10:12:27	04-09-2018 10:22:37	610 (s) 10.17 (m)	16610 16610		LP-TEST LNV808		Free Call	complete	Caller Hang up		Language: English
Securus Demo Site	HH SRPHONE	(1) 2222704652 Local		04-09-2018 12:51:25	04-09-2018 12:51:41	16 (s) 0.27 (m)	7890 7890		HELEN HUYNH	MTDOC	Free Call	complete	Called party hangup		Language: English Watched
Securus Demo Site	HH SRPHONE	(1) 2222704652 Local		04-09-2018 12:52:43	04-09-2018 12:52:54	11 (s) 0.18 (m)	7890 7890		HELEN HUYNH	MTDOC	Free Call	complete	Caller Hang up		Language: English Watched
Securus Demo Site	HH SRPHONE	(1) 2222704652 Local		04-09-2018 12:55:10	04-09-2018 12:55:39	29 (s) 0.48 (m)	7890 7890		HELEN HUYNH	MTDOC	Free Call	complete	Caller Hang up		Language: English Watched

Reports can be saved, retrieved, and shared in the following file formats:

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

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

19. Proposer shall describe their fraud control processes, to include a description of the operation of the three-way call detector. (Section C.3.1.1.Q)

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

Fraudulent calls will be the sole responsibility of CenturyLink. The CenturyLink team has spent and will continue to spend a substantial effort developing tools that eliminate fraudulent communications. Not only because of potential lost revenue for offender calls, but just as significantly by preventing an offender from having unauthorized communications with the general public and thus reducing a major security risk.

The OTS will provide, at a minimum, the following aids in preventing fraudulent use:

- Elimination of secondary dialing
- Termination of calls if a second dial tone is detected
- Prohibition of switch hook dialing and call forwarding
- A non-billed interval at the beginning of the call
- Limitation on the number of times a telephone number may be redialed by the offender within a specific period of time (parameters to be set by the Department)
- Provide a Three-Way call detector as part of the OTS
- Information such as name, address, and billing information for the called number as well as name, address and phone number or other identifying information of the person(s) prepaying minutes.
- Identification and reporting on inmate-to-inmate communication via ICER.

Constant Fraud Controls

A significant number of emerging threats are call diversion schemes that mask the true destination of calls. The OTS provides the most advanced fraud detection capabilities in the correction industry. The OTS calling service continuously analyzes call data and system parameters to detect any anomalies, hardware failures, fraud indications, or unusual usage patterns. The system logs all telephone activity and statistically analyzes it to detect attempts at call forwarding, three-way calling, 'hookswitch dialling', 'black boxing', 'hacking', and other fraudulent telephone activities.

The system, by default, does not allow the offender to press additional digits. It uses our patented DTMF collection techniques to collect and only act upon digits that the system is expecting. Unlike traditional premises-based systems, SCP controls the call and buffers digits between pressing and sending. For instance, when the system asks for language selection it expects a one-digit answer; when asking for a PIN it expects the maximum PIN length. The system does not expect digits after call connection and will not accept any extra pressed digits. This makes it impossible for offenders to receive a secondary dial tone or call anyone by dialing additional digits after call connection. This patented feature is only available on Securus' Secure Call Platform (SCP).

Three-Way Conference Calling Fraud Detection

At the discretion of the Department, the OTS can continue to direct the system to disconnect the call with messaging to offender and called party when a three-way event is detected. The OTS creates a note in the call record when this occurs. However, the OTS also provides the option of marking the call in the call record with no interruption when a three-way event is detected.

With traditional systems, offenders enlist the aid of an outside accomplice to "conference" them, via three-way calling, to an "unrestricted" line, bypassing system controls. Without three-way call detection, offenders can defeat the correctional objectives and policies of the institution and subjecting the public to offender harassment and fraud. SCP is unique in its ability to detect and defeat an accomplice's attempt to conduct the three-way event. SCP has the unique ability to

disable three-way call detection on a particular number or groups of numbers, such as main listed telephone numbers to attorneys.

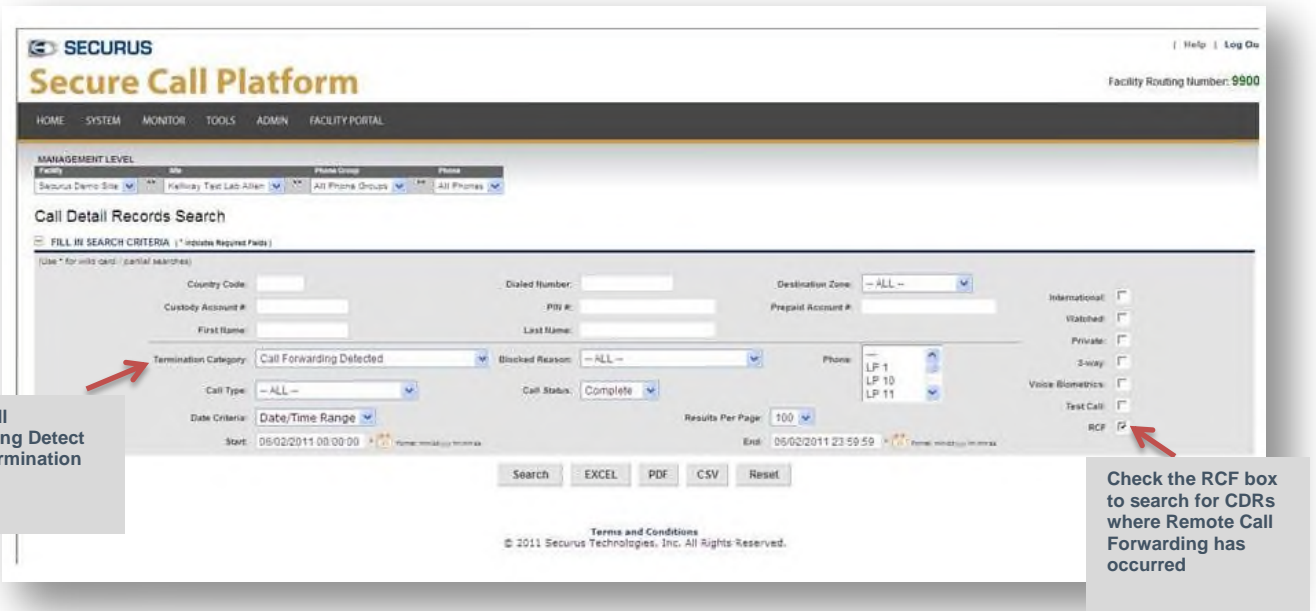
Remote Call Forwarding Detection

In conjunction with our three way call prevention system, the OTS provides Remote Call Forwarding Detection (RCFD). RCFD provides the ability to immediately terminate a call in real time if it detects that a called party's telephone number is call forwarded to another telephone number.

As an added feature, SCP can be configured to allow the call to continue with one of the two following options if false disconnects are a concern:

- Announce to the offender 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 offender and called party

The SCP user interface secure Web site provided allows authorized users the ability to create Call Detail Reports for those calls by selecting the “RCF” flag or using the specific termination code “Call Forwarding Detected” as shown in the figure on the following page.



SECURUS
Secure Call Platform

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Secure Demo Site | Halfway Test Lab Allen | All Phone Groups | All Phones

Facility Routing Number: 9900

Call Detail Records Search

FILL IN SEARCH CRITERIA (* indicates Required Fields)

(Use * for wild card - partial searches)

Country Code: [] Dialect Number: [] Destination Zone: -- ALL --

Custody Account # [] PIN # [] Prepaid Account # [] International:

First Name [] Last Name [] Phone: LP 1, LP 10, LP 11

Termination Category: Call Forwarding Detected Blocked Reason: -- ALL --

Call Type: -- ALL -- Call Status: Complete

Date Criteria: Date/Time Range Start: 05/02/2011 00:00:00 End: 05/02/2011 23:59:59

Results Per Page: 100

Search EXCEL PDF CSV Reset

Terms and Conditions © 2011 Securus Technologies, Inc. All Rights Reserved.

Enter Call Forwarding Detect as the termination category

Check the RCF box to search for CDRs where Remote Call Forwarding has occurred

ICER

As mentioned above, Securus' ICER technology provides another exceptional tool in identifying and combatting three-way conferencing. Offenders are continually finding creative ways to speak to each other using the offender phone system, and ICER listens to and identifies all of these illegal communication events. Whether two offenders are calling an accomplice on the outside who is verbally relaying messages, or the accomplice has two speakerphones to coordinate gang conference calls, ICER identifies these scenarios and proactively notifies authorized corrections staff of the event and provides details that can quickly and easily be traced back to a specific call. This call can then be listened to through Securus' industry-leading platform—SCP.



20. **Proposer shall submit a clear, concise description of the operation of the maintenance diagnostic system to include reporting of all telephones and digital recording systems to be used for Contract Monitoring purposes. (Section C.3.1.1.R)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

CenturyLink's OTS provider, Securus, exceeds this requirement in that we have an established SolarWinds Monitoring "Diagnostics" system which receives Simple Network Management Protocol (SNMP) traps (typically set for every 5 minutes but never to exceed the 24 hour test requirement) from the network equipment located at each facility which will alert the Securus Network Operations Center (NOC) of potential issues. Health thresholds and system error detection clients are established on the Secure Call Network core processing platforms at each Data Center to detect any potential issues and sends real time alerts to the Network Operations Center. The Secure Call Network transportation backbone carrier (AT&T) volume thresholds are established on core node equipment at each Data Center alerting SolarWinds of possible carrier network issues. Logs of these events are maintained for Network Operations Center for minimum 30 days and are then transferred to Lifecycle Management Servers for minimum 1 year trending reports. Diagnostic testing includes the OTS and all components such as the DRS and UPS.

The Network Operation Center is located within the Dallas, Texas headquarters of Securus. The facility is staffed 24/7 by highly trained network administrators.

In addition, the CenturyLink Team will proactively maintain the premised based equipment location at the individual Department facilities. The Field Service/Site Technicians will perform preventative maintenance to ensure that the offender telephones are in good working order. Technicians perform quarterly review of every piece of equipment including Adtrans, switches, phones and workstations. The benefit to the Department is fewer grievances from offenders, minimal interaction with the CenturyLink Team for maintenance tickets, and an all-around better customer experience.

21. **Proposer shall describe the system administrative features, functions of the proposed OTS (e.g., the system shall provide the system administrator the ability to roll the computer mouse over an Offender's list of numbers and get information as to who owns the number). (Section C.3.1.1.M)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The OTS contains highly configurable features to ensure system and data integrity. Call Detail Records and recordings will be stored in redundant data centers for a minimum of 36 months, or longer for designated records.

System Administrative Features

The information contained below includes but is not limited to the categories of the administrative feature and functions available with the OTS.

- Creating Security Templates
 - Create, Add, Updates

- User Administration
 - Create a user ID
 - Search for a user
 - Edit users
 - Reset user password
 - Deactivate a user

- Managing Job Titles
 - Create, Add, Updates

- System Administration Reports
 - Manage user authorization for reports
 - Print report lists
 - Create Excel, PDF, and CSV exports

- Management Level Settings
 - Special agency features
 - Custody account features
 - Dial to number (DTN) feature
 - Feature level management
 - Facility, telephone group and telephone features management

- Controlling Telephones
 - Maximum duration
 - Three-Way Call detection
 - Disabling telephones
 - Call length control
 - Manage call schedules
 - Create, edit , delete - call schedules

- Controlling Telephone Groups
 - Create/disable
 - Call duration
 - Three-Way detection
 - Call scheduling

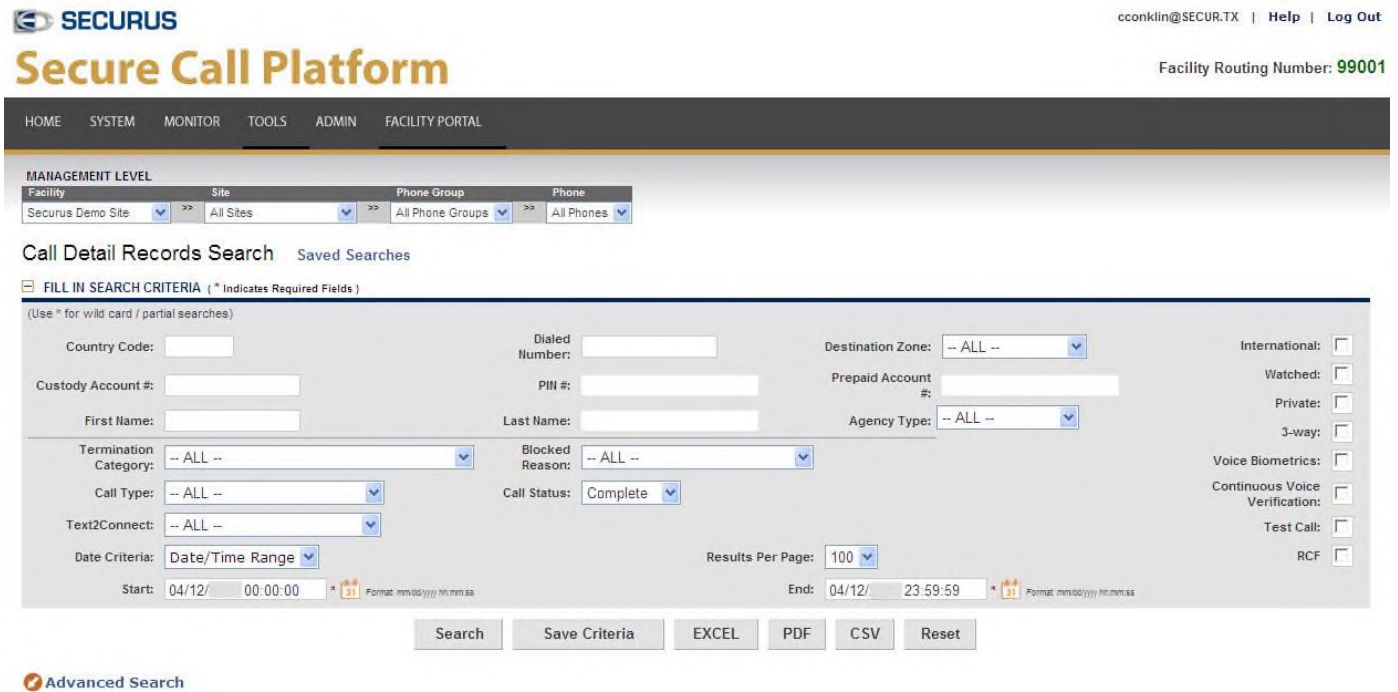
- Global Number Management
 - Allowed/denied
 - Add/delete

- Department and Facility Reports
 - Call detail
 - Call completion/attempts
 - Investigative
 - System usage

- Custody Account Control
 - Create
 - Activate/deactivate
 - Create PIN/PAN/PBI
 - Set call length
 - Set Three-Way detection
 - Assign to telephone group
 - Pre-recorded name - add/delete
 - Transfer(s) to another facility

User Functionality

Authorized users, depending on their individual privileges are able to simply navigate the SCP web based GUI. The GUI is tab based and organizes information in an easy to understand way, for example the CDR search tab enables authorized users to search CDRs using different and multiple search criteria (See search fields below).



SECURUS cconklin@SECUR.TX | Help | Log Out

Secure Call Platform

Facility Routing Number: **99001**

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Facility	Site	Phone Group	Phone
Securus Demo Site	All Sites	All Phone Groups	All Phones

Call Detail Records Search [Saved Searches](#)

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches)

Country Code: <input type="text"/>	Dialed Number: <input type="text"/>	Destination Zone: <input type="text" value="-- ALL --"/>	International: <input type="checkbox"/>
Custody Account #: <input type="text"/>	PIIN #: <input type="text"/>	Prepaid Account #: <input type="text"/>	Watched: <input type="checkbox"/>
First Name: <input type="text"/>	Last Name: <input type="text"/>	Agency Type: <input type="text" value="-- ALL --"/>	Private: <input type="checkbox"/>
Termination Category: <input type="text" value="-- ALL --"/>	Blocked Reason: <input type="text" value="-- ALL --"/>		3-way: <input type="checkbox"/>
Call Type: <input type="text" value="-- ALL --"/>	Call Status: <input type="text" value="Complete"/>		Voice Biometrics: <input type="checkbox"/>
Text2Connect: <input type="text" value="-- ALL --"/>			Continuous Voice Verification: <input type="checkbox"/>
Date Criteria: <input type="text" value="Date/Time Range"/>		Results Per Page: <input type="text" value="100"/>	Test Call: <input type="checkbox"/>
Start: 04/12/ <input type="text" value="00:00:00"/> * <small>Format: mm/dd/yyyy hh:mm:ss</small>	End: 04/12/ <input type="text" value="23:59:59"/> * <small>Format: mm/dd/yyyy hh:mm:ss</small>		RCF: <input type="checkbox"/>

Advanced Search

Another example of an easy to use SCP feature is the ability of an administrator to roll the computer mouse over a phone number in order to get information as to who owns the number (see following page).

Call Detail Records Search Saved Searches

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

302 Results PAGE 1 OF 4 >>

	SITE	PORT LOC	DIALED #	GEO LOC	START	END	DUR	ACCT # / PIN	PREPAID ACCT#	NAME	CALL TYPE	CALL STATUS	TERM CAT
<input type="checkbox"/>	Lexington County Jail, SC	BOOKING - 5	(1) 8034671426 Local		05-10-2018 00:23:26	05-10-2018 00:37:47	861 (s) 14.35 (m)				Free Call	complete	Caller Hang
<input type="checkbox"/>	Lexington County Jail, SC	BOOKING - 5	(1) 8034671426 Local		05-10-2018 00:55:33	05-10-2018 01:09:58	865 (s) 14.42 (m)				Free Call	complete	Caller Hang
<input type="checkbox"/>	Lexington County Jail, SC	BOOKING - 3	(1) 8033797588 Local		05-10-2018 00:56:57	05-10-2018 01:10:38	821 (s) 13.68 (m)				Free Call	complete	Caller Hang
<input type="checkbox"/>	Lexington County Jail, SC	C3	(1) 8033786794 Intralata/Intrastate		05-10-2018 01:03:30	05-10-2018 01:10:38	900 (s) 15.00 (m)	1030-297063		SPENCER FRASIER	AdvanceConnect	complete	Call duration exceeded
<input type="checkbox"/>	Lexington County Jail, SC	C_Pod_DWN_T1314	(1) 8439068017 Interlata/Intrastate		05-10-2018 01:04:45								
<input type="checkbox"/>	Lexington County Jail, SC	D2	(1) 8032352291 Interlata/Intrastate		05-10-2018 01:05:56								

Save selected calls to folder Add Selected to WS Queue

Name & Address Verification

PDF

Phone Number: 8034671426
 Last Verified: 05/10/2018 11:36:01
 Name: MACK WARREN
 Address: 1088 HILTON SOUND DR, CHAPIN, SC 29036-9719

View History Close

NOTE: The billing name and address information you requested could not be retrieved through traditional means. This information is the "best known" name and address information based on a third party source.

22. Proposer shall provide, in detail, their investigative software applications, services, and reporting capabilities. (Section C.3.1.1.T)

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The CenturyLink Team agrees with the Department’s investigative approach of combining data mining software with human intelligence services to aid the Department with investigations. The CenturyLink Team is fully prepared to continue to monitor phone calls at the direction of the OIG and CID. We offer a wide array of rich investigative data sources, including but not limited to Voice Biometric Identification, WCS reports, automatic import of CDR’s, JPay deposit data, and end user reverse lookup information. Most important we bring this all together into a single source for the Department – THREADS.

Of course all of this doesn’t mean anything unless you have the people to investigate and qualify all the leads generated from these data sources. Through our Guarded Exchange division, our team offers the Department valuable resources and knowledge to augment existing TDCJ investigative staff.

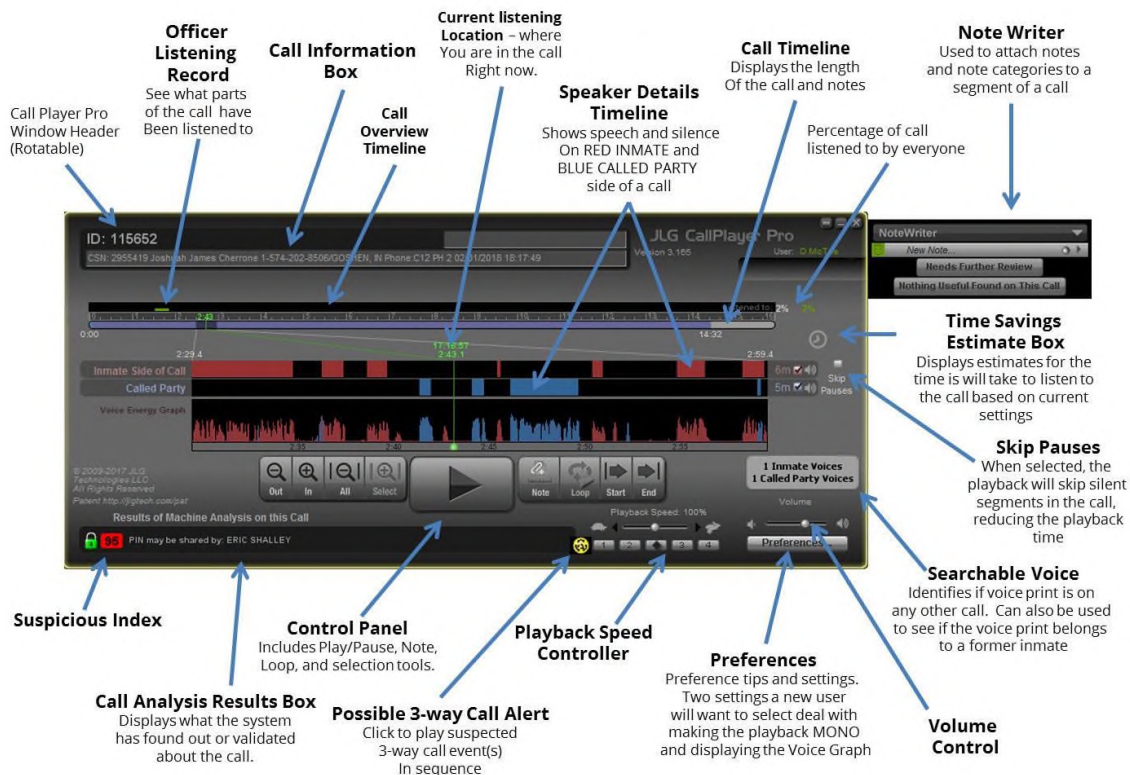


Enhanced Call Player

To allow Department staff to listen to one or both parties of a call, advance through dead space, and be able to attach notes to a recording, the CenturyLink Team provided the Department with the Investigator Pro (IPRO) Call player. The Department is currently enjoying the benefits of the IPRO call player, and can continue to do so by remaining with the CenturyLink Team.

Features of the IPRO Call Player Include:

- Ability to skip pauses to save listening time,
- Ability to mute either the offender or called party side of the call,
- A Notes feature, which allows the investigator to add a note to the entire call or to a clip in the call, and distribute notes to colleagues. The NoteWriter automatically captures the timestamp of each event and creates an audio clip that the investigator can easily attach to a note.
- Slow down and speed up playback capabilities while keeping the call intelligible,
- The “Searchable Voice” button which tells how many voices are on the call;
- Detection and flagging of calls in the analysis results box, which contains three-way call events and offender-to-offender conferences (ICER events). Investigators can pinpoint exactly where in the call the three-way or ICER event took place. The IPRO call player allows the investigator to capture a sample of a voice on either the offender or called party side of the call, save that sample, and search the entire call database for all calls where that voice occurs.



Inmate Inter-Communications Evaluation and Reporting System (ICER)

The Inmate Intercommunication Evaluation and Reporting system (ICER) detects completed calls made on the offender telephone system(s) between offenders, whether within an agency or between agencies across the country. The ICER system alerts investigators at the participating agencies of these events without transmitting any call audio.



For each offender-to-offender call ICER identifies the offenders, their locations, the call date and times, and the outside telephone number or numbers they called to make the connection.

ICER is unique in the industry in that it detects these calls even when the two offenders called separate outside telephone numbers to connect with each other.

ICER Facts:

- Installed in a fusion like environment at 1176 facilities across the United States
- Installed at 92 Counties within the State of Texas, including Harris, Dallas, Tarrant, and Travis Counties
- Over 240,000 ICER event reports generated across the United States since 2015.

How ICER Works:

1. A call “signature” representing the call and its metadata is created for each call.
2. Call signatures are encrypted and sent to the ICER servers. No call audio is sent.
3. Call signatures are compared. Matches are ICER events.
4. Each event is logged into the ICER database.
5. Email alerts are sent to investigators at the participating corrections agencies.
6. To prevent the display of protected offender data, when two facilities are involved both must provide electronic consent before details of the full report are made available.

Sample ICER Event Report:

ICER Event Report

Event Identified On: Mar 29, 2018
06:00 am (EDT)

An Inmate Inter-Communications Event has been detected involving an inmate at your facility. The details of which follows below:

Prisoner	Doe, Jane	Smith, Elizabeth
Agency	State DOC	State DOC
Site	1234	6789
Prisoner ID	3557865	3539044
Called Number	13046184141	1308675309
Station Name	RSAT DORM B PH 2	BLDG J POD A - PH 1
Call ID	18150164	18150225
Call Start Time	Mar 28, 2018 12:52 pm (EDT)	Mar 28, 2018 12:55 pm (EDT)
Time into Recording (H:M:S)	03m:16s (196 sec)	01m:46s (106 sec)
Duration of Event (H:M:S)	07m:31s (451 sec)	07m:31s (451 sec)

Link Analysis Software

Through our link analysis software—THREADS™—facility data is automatically ingested. Additional external data sources can be imported and analyzed to build an investigation. All of this takes place without purchasing any additional equipment, and it can be managed remotely at any time through an assigned Web-based facility portal. This means that the Department can access data remotely from any location that provides Internet access.

THREADS is the most widely used investigative telecommunications platform in the industry today, with more than 1.5 million offenders served, petabytes of aggregated intelligence data, and more than 2 million phone calls processed per day. THREADS' powerful data analytics engine analyzes multiple types of facility data, such as offender communication records, public phone records, billing name and address, data from confiscated cell phones, financial data, and more to automatically generate focused leads for investigators. THREADS is extremely robust and accurate, but is extremely intuitive, and easy to use —making it a perfect tool for busy investigative officers operating within a correctional institution.

THREADS automatically uploads facility data and does not require any equipment to reside on-site, saving Department Staff hours of time and energy of not having to manually upload facility data. The unique algorithms within THREADS makes what used to take an entire day of multiple officers working eight-hour shifts now just take moments.

Importing Information

THREADS will automatically import the following types of corrections information:

- Offender call records
- Offender personal information, such as name, account number, PIN, DOB, SSN, and more
- PAN lists
- Called party billing name and address information
- Video visitation
- Suspicious activity, through IPRO and ICER for example
- Financial data

THREADS can also import the following types of information from external data sources:

- Confiscated cell phones—calls, text messages, emails, videos, contacts, etc.
- Public phone records
- Events and places of interest
- Mail
- LexisNexis

Workspaces

Within THREADS, online workspaces are provided where cases can be built. These workspaces allow users to compile data and build an investigation. Pictures, locations, devices, organizations, and known associates can be inserted and attached within the workspaces to organize in-progress investigations while investigators add additional data points. Investigators can update the permissions for each workspace to allow only the active investigator, only MDOC facilities, or your full shared community to have access to individual workspaces. Through these settings, users filter editing privileges for those assigned with viewing access.

Community

THREADS further separates itself from other offender telephone service providers by providing a national community database where facilities can choose to share their data to expand and identify more investigative opportunities and leads. Facilities can choose to share data with other agencies locally, regionally, or nationally depending on their investigative needs. Through this community of data sharing, THREADS users can leverage the resources of other agencies to understand the breadth of their investigations and, therefore, close cases faster. By joining the THREADS community, users can run reports, uncover data correlations, and gather contact information unlike any other data analytics solution.

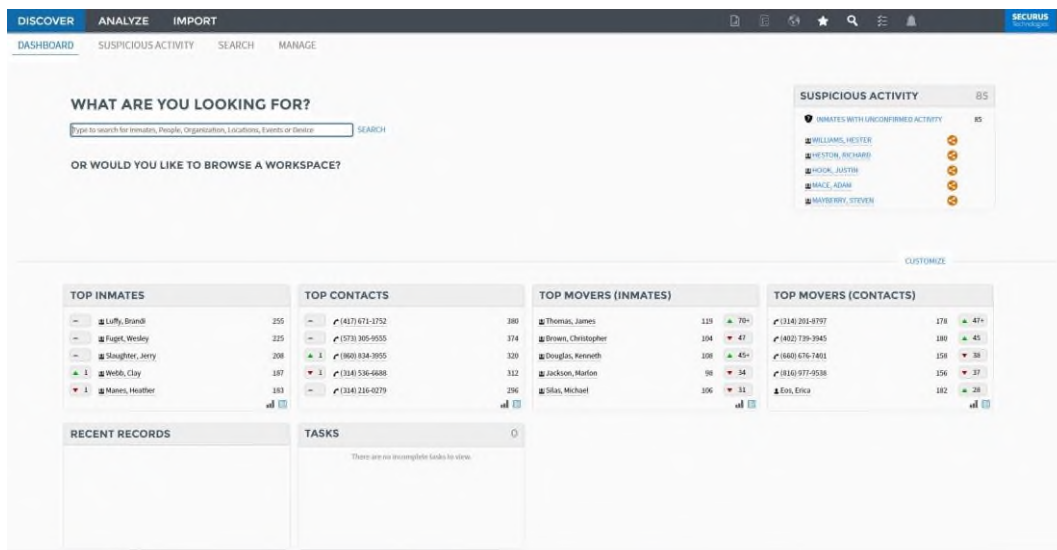
Graphic and Textual Information

All information is presented graphically as well as textually. Timeline charts and graphical analysis make it easy to reveal periods of high-intensity calling and other calling patterns on a graphical and interactive timeline.

Offender Identification and Automatic Notifications

This technology identifies the offender—even if the calls are masked by another offender’s PIN—and eliminates human intervention by receiving actionable intelligence at the push of a button. THREADS also provides automated notifications that can alert an investigator when information is found. THREADS further allows users to customize what facility information they want to appear on the THREADS dashboard in the form of investigative widgets; users can also choose which data points they want and how the information is organized.

THREADS Dashboard



THREADS Reports

THREADS provides the following types of reports:

- Statistical
- Linkage
- Working Group
- Correlation
- Time-Based
- Financial

Statistical Reports

Statistical analysis includes basic reports to start your investigation. This includes all occurrences of a phone number or a bounce list of numbers in the database and the most frequently called numbers by an offender or person.

- Identify everywhere a phone number occurs in the database, such as calls, SMS, phonebook, and BNA. This analysis can be run with a bounce list.
- Identify an offender as a potential owner of a device.
- Identify the phone numbers that an offender or person calls with the highest frequency.
- Identify all phone numbers associated with an offender or person including all calls, SMS, emails, and phonebook contacts. A bounce list can be generated from this report.
- Identify all communication details (calls, SMS and emails) between 2 or more targets or groups of targets. This report produces a CSV file for download.

Communication Activity Summary

Communication Activity on My Test List
9/21/2017 4:40:51 PM

OVERVIEW SUMMARY BY ENTITY BY NUMBER SETTINGS

OVERVIEW

We detected 1 entities related to 1 numbers in My Test List.

SUMMARY

ALL ENTITIES

Miller, Jj	1
------------	---

TARGET SUBSCRIPTIONS [CREATE BOUNCE LIST](#)

(321) 961-5629	1
----------------	---

GROUPED BY ENTITY [EXPAND ALL](#)

There are 1 entities, 1 people, related to the phone numbers and email addresses in your target list. The entries with the greatest number of relationships are displayed first.

Miller, Jj	SUB-04339	1
------------	-----------	---

We have found that 1 phone number in your target list are related to Jj. A total of 1 relationships between Jj and 1 phone number was found.

- ▶ (321) 961-5629 *Subscriber (1)*

GROUPED BY TARGET NUMBER [EXPAND ALL](#)

There are 1 items, 1 phone number, 1 email address, in your target list with relations to The items with the greatest number of relationships are displayed first.

(321) 961-5629	1
----------------	---

We have found that 1 people, is related to (321) 961-5629. A total of relationships 1 between (321) 961-5629 and the entity was found.

- ▶ Miller, Jj *Subscriber (1)*

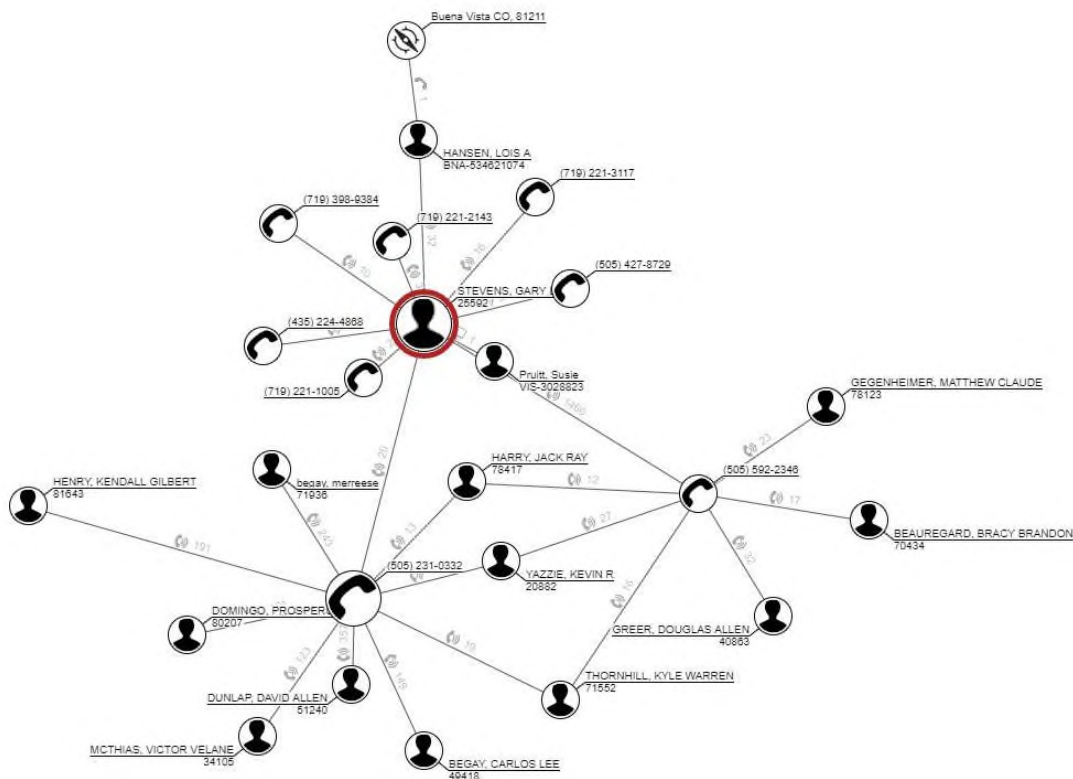
Linkage Reports

Linkage analysis shows how offenders and people are related. All the reports in this section generate graphical results that let you explore the relationships between your targets. This visual reporting tool is a quick way to understand who offenders are talking to and how the calls are related to other known numbers or offenders.

Users can generate a linkage chart that identifies:

- A target(s) relationship based on user-selected connection types, such as calls, financials, visitation, etc.
- Connections between two selected targets or two sets of targets based on user-selected connection types, such as calls, financials, visitation, etc.
- Connections between two or more targets based on user-selected connection types, such as calls, financials, visitation, etc.
- Direct relationships between selected targets based solely on phone calls

Linkage Analysis

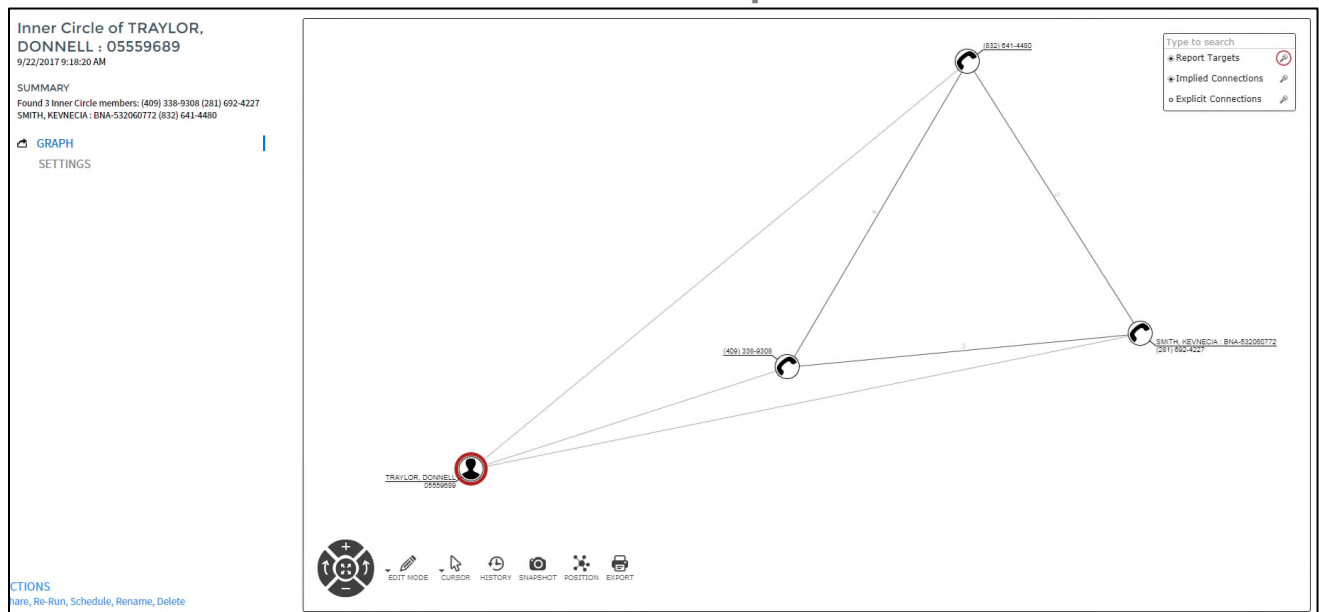


Working Group Reports

Working Group analysis uses a person’s communication behavior and calling patterns to identify phone numbers and people of interest. One of the key techniques used is temporal analysis, which associates people based on time between calls. The closer the time between calls, the more likely those calls are related. By leveraging working group reports, facilities can identify gang and other organized activity. Knowing organized groups and gangs can aid staff in monitoring member activity or even taking preventive measures against illicit activities.

- Identify a target’s “working group” or inner-circle based on their communication patterns. This report is a graphical linkage chart.
- Display a target’s inner circle changes over a predetermined time
- Show communication sequences where a target calls two or more numbers in a pattern
- Identify communication patterns—such as two or more of the same sequence—and when they occurred
- Find a target’s chain of calls. A chain is a series of calls triggered by the previous call in the chain. This report requires imported phone calls from outside the facility.
- Identify the most-likely boss in an organization based on chain analysis. This report requires imported phone calls from outside of the facility.

Inner Circle Report



Correlation Reports

Correlation analysis identifies common contacts and phone numbers between offenders, persons, and workspaces. Through correlation reporting, investigators can identify common contacts between offenders as well as fraternization between offenders and facility staff.

- Find any common communications between offenders, persons, or groups of targets
- Identify potential three-way calls between offenders
- Discover common phone numbers between two workspaces

Time-Based Reports

Time-based analysis provides reports based on the timing and frequency of an offender's or other person's communications. Find out when communication is frequently taking place, then identify periods of time where communication is not taking place. These gaps in communication can indicate behavioral changes as well as cell phone usage.

- Identify holes or gaps in an offender's or person's communication activity
- Display a set of phone numbers that a person called where communications stop with one phone number and starts communication with a different phone number within a close proximity of time. This might indicate a change of phone number or an organizational shift.
- Identify if two or more phones are being used at overlapping times. If there is a significant time overlap, it could indicate that the phones are being used by different people.
- Generate a graphical timeline of any activity—such as communication, association, financial transactions, etc.—that includes a date and time.

Hole Detection Report

Hole Detection on ESPARZA, KAREN : 01939041
9/22/2017 9:36:17 AM

SUMMARY
23 holes were found for this report.

DETAIL |

GRAPHICAL

SETTINGS

Hole Detection on ESPARZA, KAREN : 01939041

Detail

Hole Detection
9/22/2017 9:36:55 AM

Start Time	End Time	Duration
6/24/2017 12:00:00 AM	6/25/2017 4:25:36 PM	6 days 16 hours 25 minutes 36 seconds
7/1/2017 2:35:41 AM	7/6/2017 12:32:42 AM	4 days 21 hours 57 minutes 1 second
7/6/2017 2:08:59 AM	7/6/2017 11:58:49 PM	1 day 21 hours 51 minutes 54 seconds
7/17/2017 10:28:07 PM	7/17/2017 2:01:33 AM	6 days 3 hours 32 minutes 26 seconds
7/17/2017 2:08:51 AM	7/18/2017 11:57:08 PM	1 day 21 hours 50 minutes 17 seconds
7/18/2017 11:57:08 PM	7/20/2017 11:00:34 AM	1 day 1 hour 3 minutes 26 seconds
7/20/2017 11:00:34 AM	7/21/2017 1:58:41 AM	1 day 12 minutes 48 seconds
7/21/2017 1:58:41 AM	7/23/2017 11:08:13 PM	2 days 21 hours 11 minutes 32 seconds
7/23/2017 11:08:13 PM	7/26/2017 8:59:20 PM	6 days 19 hours 43 minutes 11 seconds
7/26/2017 8:59:20 PM	8/5/2017 12:15:24 AM	8 days 5 hours 11 minutes 4 seconds
8/5/2017 12:15:24 AM	8/6/2017 10:41:02 PM	1 day 22 hours 30 minutes 38 seconds
8/6/2017 10:41:02 PM	8/7/2017 11:11:41 PM	1 day 25 minutes 39 seconds
8/6/2017 2:50:22 AM	8/15/2017 1:11:19 AM	8 days 22 hours 20 minutes 56 seconds
8/15/2017 1:11:19 AM	8/19/2017 3:18:42 PM	4 days 14 hours 8 minutes 23 seconds
8/19/2017 3:22:55 PM	8/20/2017 10:41:08 PM	1 day 7 hours 18 minutes 13 seconds
8/20/2017 2:09:22 AM	8/20/2017 10:53:07 PM	1 day 20 hours 43 minutes 45 seconds
8/21/2017 2:27:08 AM	8/21/2017 4:26:30 PM	1 day 13 hours 57 minutes 22 seconds
8/22/2017 8:23:38 PM	8/22/2017 10:59:56 PM	1 day 2 hours 36 minutes 17 seconds
8/25/2017 11:00:19 PM	8/27/2017 11:47:14 PM	2 days 44 minutes 55 seconds
8/28/2017 12:01:20 AM	8/15/2017 3:05:47 PM	2 days 15 hours 54 minutes 27 seconds
8/15/2017 6:15:23 PM	8/17/2017 5:40:48 PM	1 day 23 hours 25 minutes 23 seconds

Financial Reports

Financial analysis identifies correlations between offenders and people based on the funding of an offender's accounts.

- Identify offender financial accounts with multiple funding sources
- Identify and list financial transactions of interest for a set of targets

Efficient Automated Reports

When key information is gathered, investigators must determine where all of that data will go and then take part in the time-consuming method of analysis. However, THREADS takes it one step further by allowing facilities to set up automated reports. Reports can be scheduled to take place daily, weekly, or monthly. Through this automated reporting process, users receive notifications regarding the data they use at the timeframes they select.

Managed Data Analytics

Guarded Exchange is available to assist TDCJ with THREADS reporting to help provide actionable intelligence to TDCJ facility members.

Key Word Search

The CenturyLink Team agrees with the Department's approach to investigations, combining data mining software with human intelligence to find and qualify suspicious activity. To support the Department in their investigations, the CenturyLink Team provides Word Spotting and THREADS data mining software for use in addition to Guarded Exchange services.

Word Spotting

Our Word Spotting solution was developed specifically for the corrections environment. This technology was built and tested using real calls placed by real offenders with feedback and direction from real investigators. This technology speeds up investigations, reduces labor demands and increases investigative capabilities.

SCP's Word Spotting feature includes:

- A default dictionary of more than 7,500 search words that can be customized to meet the Department's needs, including slang and jargon not found in standard dictionaries. As security threat groups expand their code word vocabulary and new intelligence is gained, new keywords can be added.
- A user-friendly interface to select suspicious offenders or phone numbers for ongoing searches.
- A Word Spotting search engine that automatically processes offenders or phone numbers with no additional involvement from facility staff.
- Integrated reporting that allows users to identify calls where specified keywords were spoken.
- 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.

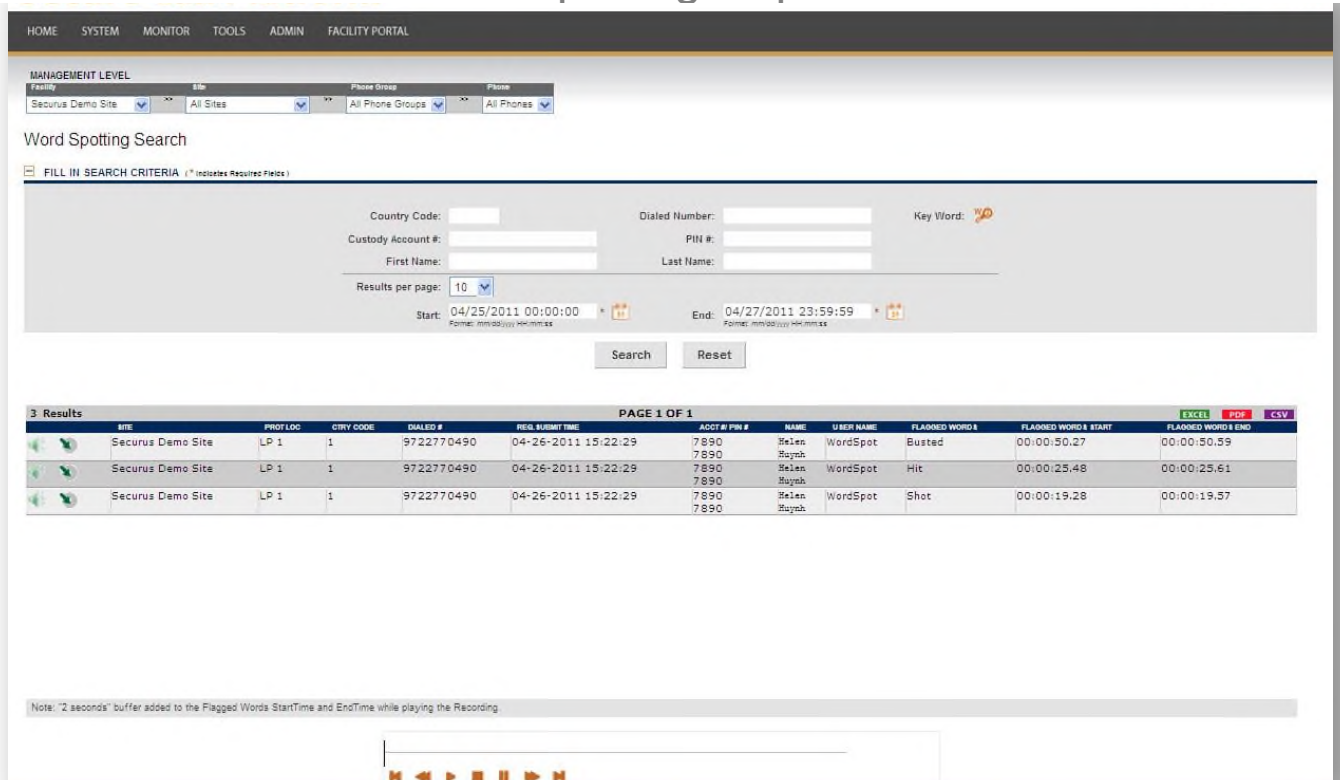
Our Word Spotting is fully integrated into the SCP platform allowing for word spotting searches for specified keywords in calls automatically without the need to switch programs or download calls.

Word Spotting Reports

Authorized users can access the Word Spotting reporting tools through SCP's user interface. Investigators use search criteria such as date range, PIN, dialed number, and offender name to pull a report that lists all of the calls with identified keywords.

The reports provide standard information such as the name of the offender, their PIN, and the dialed number. Investigators can see the identified keyword and the time within the call that the word was spoken; saving valuable time by eliminating the need to listen to the entire call.

Word Spotting Report



The screenshot displays the 'Word Spotting Search' interface. At the top, there is a navigation bar with links: HOME, SYSTEM, MONITOR, TOOLS, ADMIN, FACILITY PORTAL. Below this is a 'MANAGEMENT LEVEL' section with dropdown menus for Facility (Securus Demo Site), Site (All Sites), Phone Group (All Phone Groups), and Phone (All Phones). The main search area is titled 'Word Spotting Search' and includes a 'FILL IN SEARCH CRITERIA' section with fields for Country Code, Custody Account #, First Name, Dialed Number, PIN #, Last Name, and Key Word. There are also date range fields for Start (04/25/2011 00:00:00) and End (04/27/2011 23:59:59), and a 'Results per page' dropdown set to 10. Search and Reset buttons are located below the search criteria. The results section shows '3 Results' and 'PAGE 1 OF 1'. A table lists the results with columns: SITE, PROF. LOC, CTRY CODE, DIALED #, RECD. SUBMIT TIME, ACCT #/ PIN #, NAME, USER NAME, FLAGGED WORD #, FLAGGED WORD # START, and FLAGGED WORD # END. The table contains three rows of data for 'Securus Demo Site' with various flagged words like 'Busted', 'Hit', and 'Shot'. At the bottom, there is a note about a 2-second buffer and a media player control bar.

SITE	PROF. LOC	CTRY CODE	DIALED #	RECD. SUBMIT TIME	ACCT #/ PIN #	NAME	USER NAME	FLAGGED WORD #	FLAGGED WORD # START	FLAGGED WORD # END
Securus Demo Site	LP 1	1	9722770490	04-26-2011 15:22:29	7890	Helen Hayek	WordSpot	Busted	00:00:50.27	00:00:50.59
Securus Demo Site	LP 1	1	9722770490	04-26-2011 15:22:29	7890	Helen Hayek	WordSpot	Hit	00:00:25.48	00:00:25.61
Securus Demo Site	LP 1	1	9722770490	04-26-2011 15:22:29	7890	Helen Hayek	WordSpot	Shot	00:00:19.28	00:00:19.57

Word Spotting Keyword Management

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL
Facility
Securus Demo Site

WS Triggers **Keyword Management**

KEY WORD MANAGEMENT

The keyword you have selected to be added will only be applicable against recordings which are flagged after adding the new keyword. Previous applied recordings will need to be run again manually to search for the word. *You can check Word Dictionary under the Online Help when you want to create and add a word to your selected list.

Look for: Keywords 🔑

Available Keywords

Selected Keywords

Add > < Remove

*Delete *New Keyword

*Words created by you can be deleted from Available Keywords only

Update Reset

Word Spotting Search Configuration

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL
Facility
Securus Demo Site

Word Spotting Trigger Summary

WS Triggers **Keyword Management**

WORD SPOTTING CONFIGURATION

Trigger	Selected
Custody Account	45
Phone Number	36
Available CDR: 250	0

REMOVE PHONE NUMBER TRIGGER

36 Results PAGE 1 OF 4 >> EXCEL PDF CSV

<input type="checkbox"/>	COUNTRY CODE	PHONE NUMBER	LEVEL	DETAILS	TRIGGER-SET USER NAME	TRIGGER-SET DATE/TIME
<input type="checkbox"/>	1	9722770668	PAN	24680/24680	Chuong Dang	12-19-2012 04:12:30
<input type="checkbox"/>	1	9722770668	Global - Site	Kellway Test Lab Allen	Jose Castro	11-17-2011 17:11:16
<input type="checkbox"/>	1	2142044321	PAN	9722770668/2770668	Lester Disney	11-17-2011 10:11:12
<input type="checkbox"/>	1	2142023794	PAN	3011/2021	Dean Ramsey	11-12-2012 13:11:05
<input type="checkbox"/>	1	7894321123	Global - Customer	All Sites	Dee Sonti	11-10-2010 04:11:58
<input type="checkbox"/>	1	9722770668	PAN	9087032071/201009087	madhu boddu	11-10-2010 02:11:10
<input type="checkbox"/>	1	9722770668	Global - Site	Production Support	madhu boddu	11-10-2010 02:11:09
<input type="checkbox"/>	1	2345678901	Global - Site	Production Support	Lester Disney	11-09-2011 15:11:28
<input type="checkbox"/>	1	9722770668	PAN	00099887768/099887768	Dee Sonti	11-04-2011 08:11:47
<input type="checkbox"/>	1	9722770668	PAN	191013/7604	Bryan Carrell	11-03-2011 15:11:23

Remove Trigger

Analytical Services through Guarded Exchange (GEX)

As stated previously, the CenturyLink Team agrees with the Department's investigative approach of combining data mining software with human intelligence services. Currently Guarded Exchange (GEX) is working priority requests from the Department and producing Suspicious Activity Reports (SAR's) for approximately 15,000 monthly offender calls. We offer to continue these services in order to meet or exceed this requirement. In addition, we offer expanded Guarded Exchange services in our response to Section C.3.10 – Added Value.

Through GEX, we have been providing experienced, certified, professional personnel to provide monitoring of calls longer than any other vendor. As such, we have developed tools and processes that are refined and proven to be effective in large scale DOC environments.

We urge caution in this category as the promise of monitoring calls cannot be effectively achieved without experience and full integration with your investigative suite of tools.

Effective call monitoring is a function of the number of personnel available to listen to calls, to the level of comprehensive understanding of what your investigators are looking for in calls and having full integration into your investigative software and systems so that “actionable intelligence” derived from calls can reach investigators in a timely manner.

Through Guarded Exchange, we will provide a sufficient number of personnel to listen to the required number of calls. Offender calls to be monitored will be based on the use of proprietary data mining, behavioral analysis and filtering technologies and other proprietary strategies in conjunction with the intelligence gathering priorities established by the Department.

The monitoring will use a combination of technology from Guarded Exchange and Securus and sufficient personnel for the purposes of collecting intelligence from the Offender Telephone System.

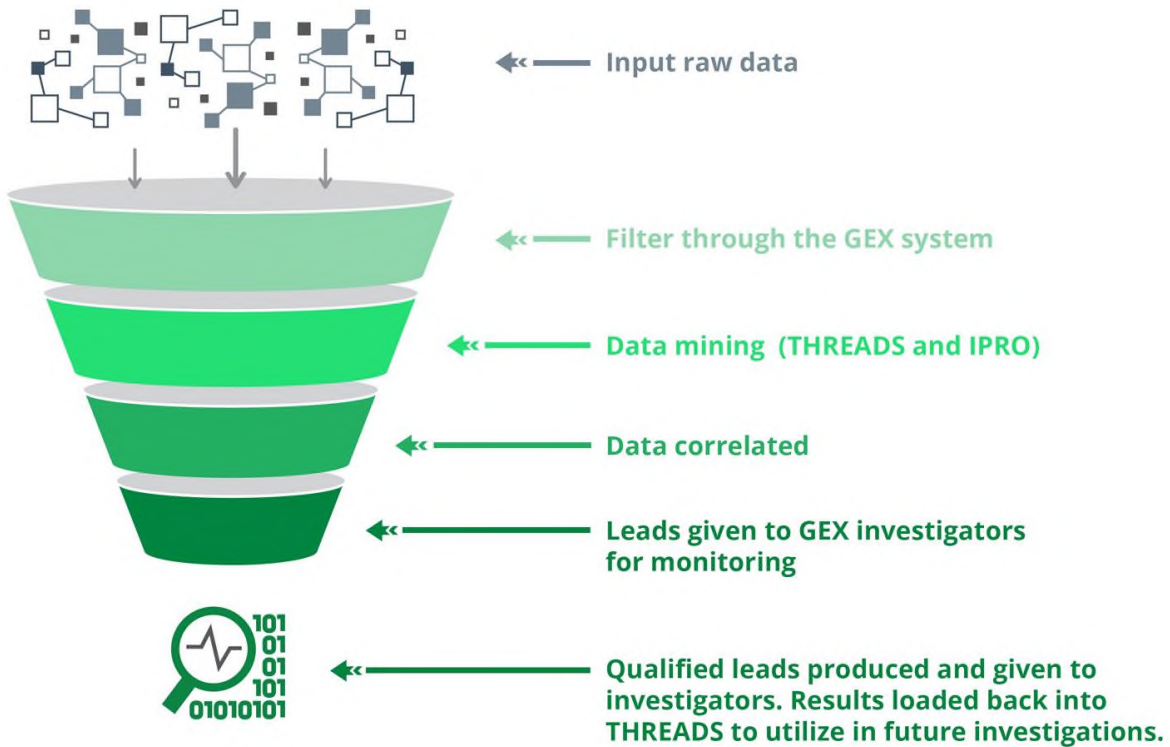
The use of these, trained personnel, proven strategies and technologies will identify at a minimum the following:

- Suspicious or suggestive key words or phrases
- Calls that suggest threats to the safety and security of the facility, staff, volunteers, and offenders entrusted to the care of the Department
- Criminal activity inside and outside of the facility

Since July 2017 GEX has monitored 164,906 calls through April 2018, including the review of 431 ICER events.

The CID and OIG have made 13 separate requests for GEX assistance looking for any intelligence regarding the introduction of narcotics, drug activity, drug use, Inmate and Staff Relationship, nefarious activity, transcriptions regarding a murder, saturations of 3 separate housing units, STG information and translation of Spanish calls.

GEX has provided a total of 204 Intelligence reports to TDCJ.



GEX provides a comprehensive suite of investigative products and is the industry leader in intelligent monitoring of offender calling. The GEX solution includes the most advanced technology available integrated into a single, cohesive system whose sole purpose is to aid agencies in generating Actionable Intelligence™.

The GEX solution includes:

- Live Monitoring of Calls via dedicated personnel
- 70 proprietary technologies that allow GEX to data-mine through millions of phone calls, emails, financial transactions and other information sources providing intelligence that counts.
- Licensed Private Investigator Staffing to ensure that trained, professional personnel are the ones aiding in the investigations.
- Proven Experience that can only be achieved through time tested processes and solutions - GEX has monitored over 1.1 Million Calls and this number grows every day. No other vendor can match Guarded Exchange's experience.

Guarded Exchange Investigative Monitoring Services will provide the following benefits to the Department:

- Increased staff, offender and public safety and security
- Increased investigative efficiencies
- Development of actionable intelligence


Software and Service Generated Reports

As TDCJ's current OTS solution provider, the CenturyLink Team has already developed and/or modified many of our system software and service generated reports to meet the needs of the Department. In addition to those reports, which are described in detail in Answer #13, the CenturyLink Team also provides in-depth, investigative intelligence on TDCJ offenders through our Guarded Exchange Investigative Support service.

While daily monitoring of calls is a primary goal and activity, upon request from the Department, the CenturyLink Team can redirect personnel to a targeted subset of calls with the ability to monitor and report on thousands of calls in a matter of hours or days in order to support a specific investigation and/or threat, such as escapes, disturbances, and gang/STG activities.

The results of an offender investigation are provided to the Department in the form of a Suspicious Activity Report (SAR) along with all Actionable Intelligence gathered from the discovery process. An example of this report is provided on the following page:

Sample GEX Report



Guarded Exchange
 2728 Plaza Drive Suite B
 Jefferson City, MO
 guardedexchange.com

SUSPICIOUS ACTIVITY REPORT

GEX Tracking Number: Report Date:

GEX Staff Assigned: Incident Location:

Incident Date/Time:

No Photo Currently Available	Subject# 1	Title, Name, DOC# (Last, First, Middle): Inmate [REDACTED]	Height: [REDACTED]	Weight: N/A
	Type: Suspect	Race: [REDACTED]	Gender: Male	Status: N/A
[REDACTED]				
No Photo Currently Available	Subject# 2	Title, Name, DOC# (Last, First, Middle): Unknown	Height: N/A	Weight: N/A
	Type: Suspect	Race: N/A	Gender: Male	Status: Civilian
[REDACTED]				

Address: [REDACTED]

Information found on the Offender Phone System is indicative that Inmate [REDACTED] may be conspiring with a male civilian to introduce "three or four" unknown controlled substances into [REDACTED] via mail.

Escalated Call:
 08/30/2016 @ 11:19:06 This is believed to be Inmate [REDACTED] speaking with a male civilian at telephone number [REDACTED]

At CP 01:15 The civilian refers to Inmate [REDACTED] as "[REDACTED]"

At CP 01:18 The civilian says, "I just got off the cell phone with [REDACTED]. He going...he going to pick it up and I'm going to go meet him, go to his crib, go get about three or four." Inmate [REDACTED] says, "Alright alright." The civilian says, "I just talked to him off my phone before you called." Inmate [REDACTED] says, "Alright alright...appreciate it pops. Listen, you hear me? Um...when you get it um...just...just just...you can do it how um...I wrote you in the letter, you hear me?" The civilian replies, "Yeah." Inmate [REDACTED] continues to say, "Cause...you ain't got to...you ain't concealing nothing...as far as the..." The civilian says, "Okay, I hear you." Inmate [REDACTED] says, "And that'll be that, you know? But you ain't got to go do nothing extra cause you have envelopes there, right?" The civilian replies, "Yes." Inmate [REDACTED] says, "Yeah...and everything else..." The civilian interrupts to ask, "The big ones or the little ones?" The civilian says, "Nah the little ones...the small joints." The civilian says, "Alright."

At CP 02:13 The civilian asks, "Leave 'em in the pack or take 'em out?" Inmate [REDACTED] replies, "Take 'em out." The civilian says, "Alright got you." Inmate [REDACTED] says, "Just divide it by how I told you to, you know what I'm saying? Cause it...the um...it should be...it should have the numbers on there, know what I mean?" The civilian says, "Okay."

Note:
 A search of the escalated number in specific resources lists the number to "[REDACTED]" at address: [REDACTED]

23. Proposer shall describe, in detail, their eMessaging solution, the hardware, and reporting capabilities. (Section C.3.1.1.U)

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

As TDCJ's current provider of eMessaging services, the CenturyLink Team knows first-hand what works for the Department and how to implement the perfect system that continues to meet TDCJ's needs. The JPay (now part of Securus) eMessaging system already has printers, associated hardware, and a robust online eMessaging management and reporting system in place to handle the specific requirements stated above.

This same system is installed at 18 state Departments of Corrections across the country. Hundreds of thousands of users have sent and received tens of millions of emails, photo and video attachments, and eCard greetings.

Family and friends access this service online at JPay.com, including from the JPay iPhone and Android mobile apps in order to send a message to their TDCJ loved one. Since the Department currently does not allow outbound messages and photos, we have customized its eMessaging system to accommodate TDCJ policies. All inbound messages and photos are printed out and delivered to offenders after facility staff have reviewed and approved via our secure online management portal, the Facility System.

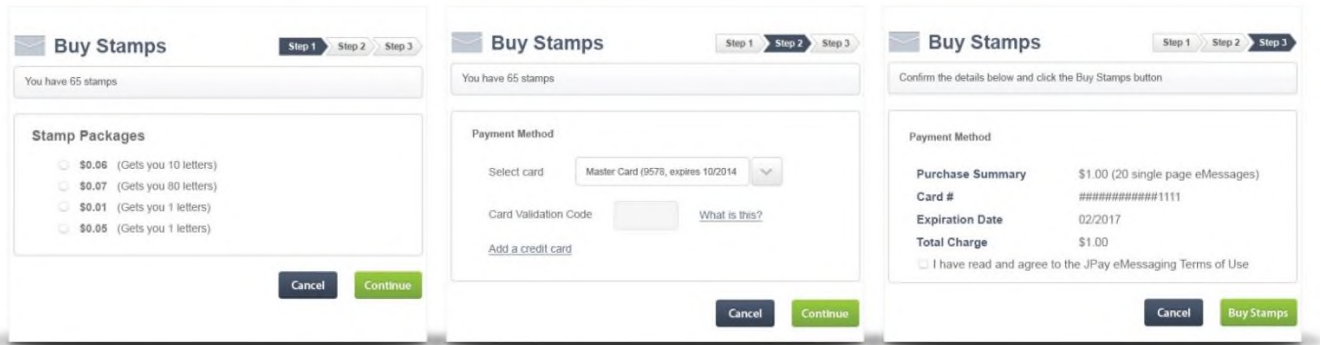
All messages are paid for with virtual stamps, which are available in bundles. Stamp purchasing is simple and never interferes with composing and sending of email messages. With our email system in place, facility staff no longer needs to expend valuable man-hours examining letters for inappropriate content or contraband. Valuable staff resources can now be redirected to more urgent issues, as computer systems take on the task of analyzing incoming correspondence. Over the years, this system has been instrumental in a handful of recaptures, stopped many messages that were STG threat-related, deciphered many encoded messages, and much more.

Stamps

Customers buy and use virtual stamps to send emails, photos, and eCards through the service. Customers purchase stamps on the web site and on their mobile device using a credit/debit card. A one-page email (about 5,000 characters) costs one stamp. Longer messages require additional stamps and customers are asked to confirm extra stamp expenditure before sending the email. Each added recipient also adds one stamp to the cost.

Buying stamps on JPay.com

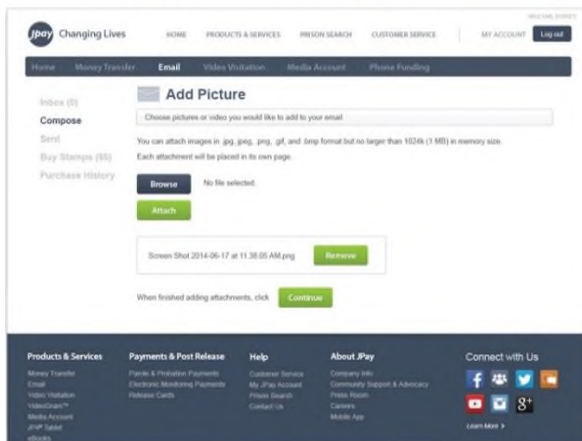
To purchase stamps on the web, the user simply selects a stamp package to purchase from the Stamps section in the user menu. The user can choose from three bundles when purchasing stamps, depending on their anticipated usage. Stamp costs for TDCJ customers will continue to be fixed at the current price of a first class postage stamp, just as they are today. As soon as the transaction is completed, the customer can begin sending emails.



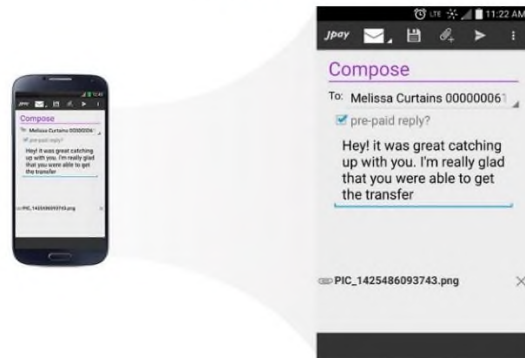
Buying Stamps via the App

Just like the website, the customer must have stamps in order to send email from the app. To buy stamps, the customer chooses a stamp package, selects and confirms the payment method and taps "Purchase."

Attach a photo to your email



Include an attachment on your smartphone



Email Review and Approval

All incoming email is routed to the Facility System for staff review and approval before release. Each email is automatically screened for content and if certain criteria are met, the message is flagged for special review. Even if a message has no questionable content, the Department can still hold each message for review and approval before it is released to the mailroom for printing.












How It Works

The flagged email review process is in place at 18 state correctional agencies. As a result, their investigators get accurate and relevant intelligence and their mailroom staffs are not bogged down reviewing and approving emails that do not pose a security threat.

Once a word list is set, we monitor the flow of emails and continually provide the Department with metrics on the frequency and type of words being flagged. For example, the word "kill" seems to be a likely inclusion in a flagged word list, but it actually does not provide valuable intelligence because it is part of many common expressions such as "kill my appetite" or "just killing time" and appears in more than 10% of all email traffic. In fact, it actually hampers the mailroom's ability to identify and escalate real threats and delays the delivery of email. Conversely, seemingly innocent words such as "disciple" or "greendot" often appear in letters referencing criminal/gang activity.

Flagged emails require staff approval before being delivered to the recipient's inbox. All messages containing attachments are automatically flagged for review. Messages are then presented in "Buckets" depending on status. For example, all messages that contained words flagged by the dictionary or user watch lists would reside in the "Requires Approval" bucket as shown below.

Letter Delivery

Inbound	Outbound
 Requires Approval (190) Click to view letters pending approval	 Requires Approval (3) Click to view letters pending approval
 Ready To Print/Release (2867) Click to view, ready to release and ready to print letters	 Ready To Print (1) Click to view, ready to release letters
 Printed (0) Click to view and reprint printed letters	 Released (N/A) Click to view released letters
 Released (N/A) Click to view released letters	 Sent To Security (N/A) Click to view and approve letters sent to security
 Sent To Security (N/A) Click to view and approve letters sent to security	 Censored (N/A) Click to view censored letters
 Censored (N/A) Click to view censored letters	

An email auditing feature tracks all staff activity so supervisors can see who approves and releases individual messages. Emails can be flagged for various reasons such as:

- Word List - Flagged because a word from the "flagged word" list was used
- Watch List - Flagged because an offender or customer is on a watch list
- Contains a photo attachment

The CenturyLink Team will work continue to work closely with TDCJ staff and investigators to ensure the Department keeps reaping all the benefits of these investigative capabilities.

Approval Process

Approved facility staff can either release the message to the mailroom for printing or request additional review. Typically, agencies predetermine who performs any additional review of an email to determine if it is a security threat. That team, usually investigators, can release the email or return it to the sender. In addition, the email can be indefinitely detained or discarded entirely. The user has the option to notify the customer and/or offender if and why the message was discarded.

To save time and keep the mailroom operating at the highest levels of efficiency, the system includes an "Approve All" feature. If messages pass the screening process and are not flagged by a watch list, the messages can be automatically released for printing.

Editable Dictionary

Facility staff can pre-populate the system with words, key phrases, or character strings that flag and restrict an email from being released for printing until it is reviewed. Staff members can manage the word dictionary and user watch lists, or have JPay administer the system. All changes occur in real time and are populated system-wide instantly. Entire dictionaries, single words or phrases, suspicious offenders, or customers can be established statewide or shared by region or by facility.

Word Filtering Page

Word (s) to Appy
[Add+](#) | [Search](#)

Facility

Word	Active Since	Facility	Status
Gallo	12/20/07	Wisconsin Prison	ACTIVE
Gang	12/04/07	Wisconsin Prison	ACTIVE
Ganga	01/08/12	Wisconsin Prison	ACTIVE
Gangsta	11/29/13	Wisconsin Prison	ACTIVE
Gangstah	12/02/07	Wisconsin Prison	ACTIVE
Gangster	12/02/07	Wisconsin Prison	ACTIVE

Watch Lists

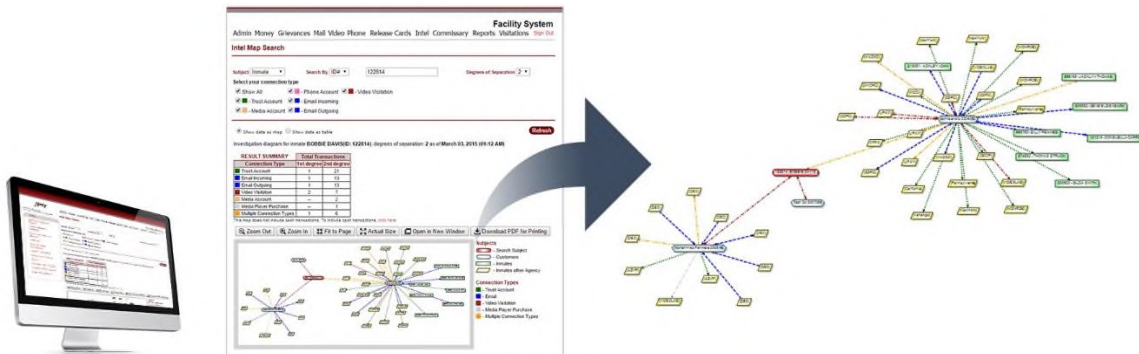
When a customer sends an email, our system scans it for customer or offender names on a predefined, customizable watch list. An alert is automatically sent to the agency investigator via email, detailing the customer name, offender name, and ID. The investigator can then approve or deny the message accordingly, depending upon TDCJ parameters.

Facility staff can easily place any offender or customer onto a watch list. The Department can add customers to a watch list for specific products such as email or a combination of products such as money and email. Facility staff can customize their own alerts based on offender and customer activity. For example, a staff member may choose to receive an alert if multiple offenders are receiving email from one customer. The system will alert the staff member via email whenever this customer uses our system to send money or emails to an offender. This represents an unprecedented level of detection capability for TDCJ staff.

Snap n' Send

Another innovation for offenders and their friends and family is our new Snap n' Send feature on the JPay mobile app. It lets customers take and send a photo to their incarcerated loved one in a single, intuitive step, similar to other popular photo-sharing apps. Since it integrates with our existing secure email system, it retains all of the security benefits of email photo attachments while streamlining the process of sharing images. Snap n'Send photos are reviewed, approved, and released for printing in the same manner as email and photo attachments.

Reporting



JPay provides a robust reporting feature for facility personnel through our secure online management portal called the Facility System. In addition to the wide selection of pre-formatted reports that already exist, JPay will work with the Department to develop specific customized reports. Reports are available in a number of formats such as XLS, RTF, and PDF. The Facility System is accessible from any computer with an internet connection and uses two-factor authentication for users, making access both role-based and limited by facility. The Department determines which personnel have access to the Facility System and then administers access through discrete user groups. This feature, for example, could limit mailroom staff access to Facility System functionality that deals specifically with electronic messaging.

User rights are tailored to each staff member, though staff members with similar rights can be granted custom levels of access via our user group feature. Authorized staff can add users to a group without having to recreate individual permission sets for each user. Even if a user is assigned to a user group, TDCJ administrators can tailor that user’s access level.

Drill-down reports are available on all clickable items found in the Facility System. For instance, a TDCJ user can click on an offender’s name to instantly see all of the eMessaging activity conducted by that offender over a defined period. A few examples of existing reports include the following:

Frequency Report

Frequency reports show the user how often a customer or offender is sending or receiving mail. This report can be run for any range of dates. The system identifies all offenders who received messages during the period entered into the search parameters. The offenders who received the most email messages are listed on top allowing the officer to immediately identify those receiving an unusually large amount of communication in a short time period.

Suspicious Criteria Report

This tool allows TDCJ users to set up criteria in order to receive email alerts. The user is sent an email if the criteria gets a match. Select a "Feature" and choose whether to receive alerts for activity related to offender payments or offender email. Select a "Scope" to receive alerts for activity related to a specific offender, a specific customer, a specific housing unit, or a specific facility. Select a "Specific Customer" to receive an alert for activity that is related to a specific customer. For example, if the user selects "Feature – Money, Scope – Agency, Specific Customer – No," then the user receives an alert every time someone sends money to any offender in the state.

Suspicious Criteria Report

This is where you can set up criteria to receive alerts via email. Select a "Feature" to receive alerts for activity related to money transfers, electronic mail or video visits. Select "Scope" to receive alerts for activity related to a specific inmate.

Page 1 of 1

Feature	Scope	Word or Phrase	Value	Specific Customer	Customer #	Delete
All	Agency		--	NO	--	Delete
Jvisit	Facility		S_500022	NO	--	Delete

Intel System

An incredibly useful tool available within JPay’s Facility System is the Intel System, which includes search functionality and reports that enable investigators to detect offender and customer linkages, identify suspicious activity, set up multiple alerts, and graphically map all data for easier analysis.

Router Detection

One important feature available through the Intel System is called Router Detection. This enables TDCJ investigators to identify customers or offenders who communicate with a specified number of people. Conversely, the user can search for a list of all offenders who received communication from more than eight different customers. From either list, the user can click any one of the offenders or customers listed in the search results, and the system will display all relevant customer and offender data.

Router Detection

- Inmates
- Customers

Show all customers with more than direct linked inmates

- Without Cash Transactions
- Include Fraud Transactions

[View Senders](#)

Customers with more than 8 direct linked inmates

Customer	Customer ID	Num of Direct Connections	
Sheila Howard	1038971	8	show network
Antoinette Chambers	1038972	8	show network
Julie Proveaux	1038973	8	show network
Dorothy White	1038974	8	show network
Patricia Ghoens	1038975	8	show network

For comprehensive searches and sorting, users can export search results to MS Excel.

	A	B	C	D	E
1	Level 1 Intel Network Data for ID .Date Created:2/27/2017 2:28:08 PM				
2					
3	From (ID)	From (Name)	To (ID)	To (Name)	Link Type
4	17028129	Alicia Burdick	83667	STEVEN RUSSELL	Inbound Mail

In-Depth Search Ability

Facility staff can also look up specific transactions or the complete history of an offender or customer's activity. Transactions can be searched by any of the following criteria:

- Offender first, last, or full name
- Offender ID
- Customer first, last, or full name
- Customer account ID
- Customer IP address
- Batch number
- Transaction number
- Customer phone number

As an example, if a TDCJ user chooses to search by customer, the submenu provides the ability to search by the customer's first name, last name, full name, account ID, or IP address.

Cross-Jurisdictional Analysis

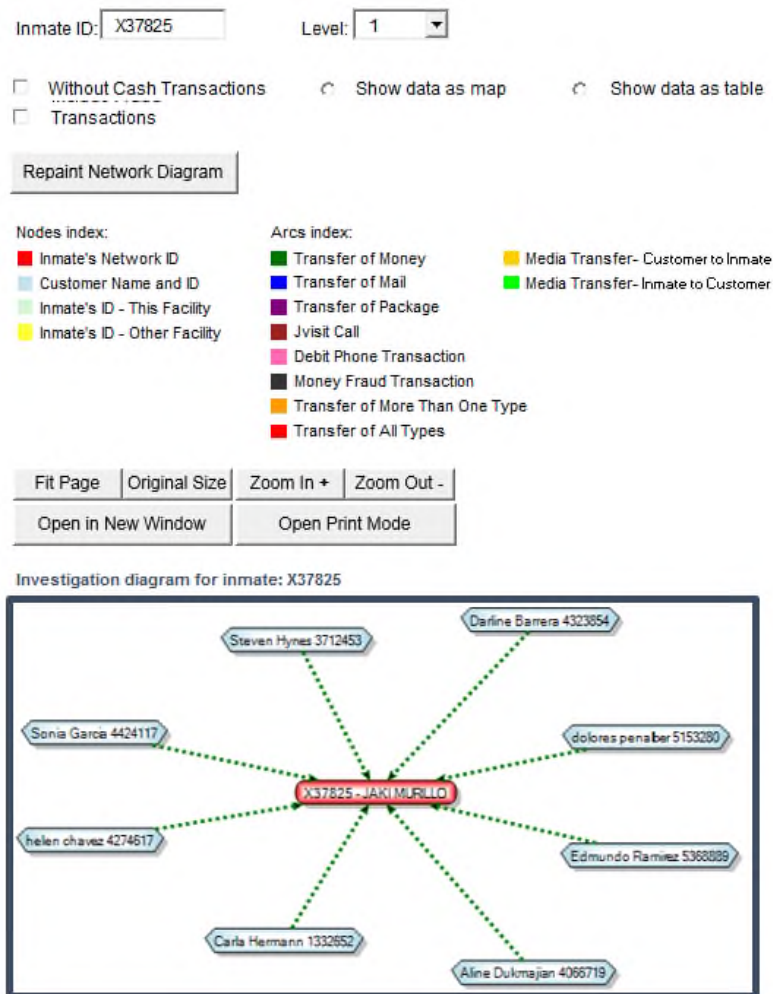
JPay currently works with more than 30 state correctional agencies and numerous county agencies around the country, including TDCJ. In compliance with each agency's rules and regulations, JPay shares many jurisdictions' data with other system users to generate cross border investigation results. This data sharing has been a tremendous success for bordering corrections agencies.

During an investigation, Department investigators may require detailed information about transactions that occurred outside their jurisdiction (typically TDCJ transactional data). On more than one occasion, gang activity has been uncovered using this shared information.

JPay's intelligence capabilities include the ability to view multiple degrees of separation in terms of offender/customer relationships. The graphical map can display complex networks of associations between offenders and customers, not just direct contact (communication or funds transmission). The system is configurable to display as many degrees of separation as the Department prefers.

Graphical Mapping

What used to take investigators countless hours is now performed with the click of a button using a quantity of data far greater than any human can analyze. With the Intel Mapping feature, investigators can quickly see an offender or customer's transactional network, saving hundreds of hours of analysis. TDCJ investigators can use this tool to identify gangs or other Security Threat Groups. In addition, financiers or other members of the group on the outside are identified and their full transaction history is at the investigator's fingertips. This system has repeatedly proven itself in correctional agencies nationwide.



24. Proposer shall describe, in detail, their video visitation solution between Department locations from friends and family to Offenders at their assigned unit. (Section C.3.1.1.V)

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The CenturyLink Team is proposing a video visitation solution to the Department that enables TDCJ offenders located in one unit the ability to participate in a video session with their friends and family members located at a different unit. These on-site video visits will be offered at no cost using the Securus Video Visitation (SVV) solution, a centralized visitation platform similar to the Secure Call Platform (SCP) offender calling system.

The SVV solution lets family and friends schedule a video visit, in advance and subject to approval by the Department, and then travel to one of the six (6) TDCJ visitor sites listed below for their visit with the offender.

The CenturyLink Team is committed to delivering this capability to TDCJ offenders and will work closely with the Department to determine the best approach to minimize TDCJ staff involvement. The units identified in this solicitation for the video visitation solution include:

Visitor Site	Offender Site
Houston - Jester III	Amarillo - Clements
Beeville - Garza Complex	Kennedy - Connelly
Dallas - Hutchins	Gatesville - Crain
Lubbock - Montford	Tennessee Colony - Michael
Austin - Travis	Beaumont - Stiles
El Paso - Sanchez	Huntsville - Wynne

The proposal includes deployment of 10 video visitation stations at each of the 12 facilities, for a total of 120 visitation terminals.

Onsite visitation

All onsite video visits must be approved by the Department. Once a visit is scheduled, the Department will have access to either approve or deny the visit through the SVV application. Once approved, a daily report will be generated and sent to a designated point of contact at each offender visitation site in order to notify the offender of an upcoming video visit.

Family and Friends can schedule their onsite visitation in two easy ways:

- Visiting www.videovisitanywhere.com through a mobile device or computer
- Securus mobile app: Visitors can schedule an onsite visit by downloading the Securus mobile app to schedule the next onsite visit

When a visitor arrives at a facility for a video visit, they will be directed to the designated video visitation terminal area after passing through security. Once at the touch-screen video visitation terminal, the visitor will enter a PIN unique to that visit as validation of the visitor’s appointment with the offender. The PIN is provided to the visitor after scheduling the onsite visit.

Once the offender gains access to the video visitation terminal, they will open the appointment page to locate the scheduled visit. The offender must then enter in his/her PIN to join the visit. The offender must also acknowledge that the visit will be recorded and monitored.

The visit is connected once both parties have entered their PINs to join the video session. All visits are scheduled for a specific timeframe and the countdown timer for the visit begins at the designated start time of the visit, regardless if the visitor or the offender has joined. All visits are recorded and there are a number of reporting tools to assist with administration of the SVV as well as for information on investigations.

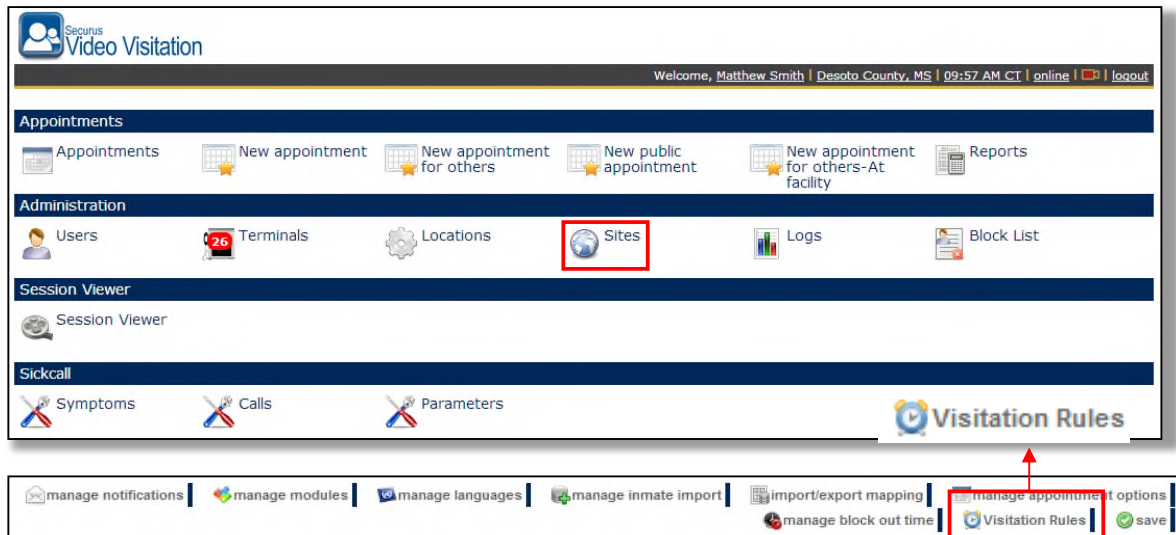


Efficiency-Driving Administration

Visitation Rules allows for the creation of quotas for the frequency of visitation by user, terminal, location, user group, and site. This feature allows the Department to create and enforce rules and policies.

Visitation Rules are accessed through the SVV application at <https://securusvideovisitation.securustech.net/>. Select the “Sites” icon, and then choose “Visitation Rules” from the bottom navigation bar. Other items accessible only by SecurUS administrators appear in the bottom navigation bar such as “manage modules.”

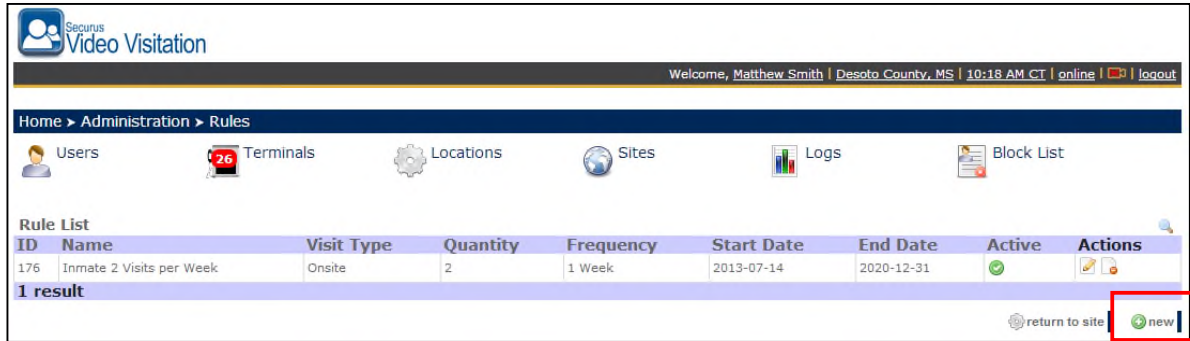
Visitation Rules





Creating New Visitation Rules

While in the Visitation Rules section of the SVV portal, click on “new” to create a new Visitation Rule.

Create a New Rule



The screenshot shows the 'Securus Video Visitation' portal interface. The user is logged in as Matthew Smith from Desoto County, MS. The navigation menu includes 'Home > Administration > Rules'. Below the menu are icons for 'Users', 'Terminals' (with a red '26' badge), 'Locations', 'Sites', 'Logs', and 'Block List'. The main content area displays a 'Rule List' table with the following data:

ID	Name	Visit Type	Quantity	Frequency	Start Date	End Date	Active	Actions
176	Inmate 2 Visits per Week	Onsite	2	1 Week	2013-07-14	2020-12-31	<input checked="" type="checkbox"/>	 

Below the table, it indicates '1 result'. At the bottom right of the table area, there is a 'return to site' link and a 'new' button, which is highlighted with a red box.

From here, you will define a rule name, and configure the following fields:

- Visitation Type:
 - Regular: Unpaid remote visit
- Quantity: Maximum quantity of the selected visitation type
- Frequency: Frequency of duration of time
- Duration: Day, Week, or Month
- Start Date: Date in which the Visitation Rule will begin to be enforced
- End Date: Date in which the Visitation Rule will end. Rules will continue to be enforced on the end date and will discontinue the following calendar day
 - All Visitation Rules MUST have a start and end date
- Status: While creating a new rule, the “Activate” checkbox must be selected for the rule to be active. Existing rules can have a status of:
 - Active
 - Disabled
 - Expired

Define a New Rule

New Rule

General

Rule Name:

Visit Type: Regular

Quantity:

Frequency: 1

Duration: Day

Start Date:

- For weekly rule, the start date must be the first day (Sunday) of a week.
- For monthly rule, the start date must be the first day of a month.

End Date:

Status

Active:

Add Associations

User

More

To search a user, enter the first name OR last name OR user name OR JID, then click search button (magnifier icon).

Terminal

More

To search a terminal, enter the terminal name, then click search button (magnifier icon).

Location

More

To search a location, enter the location name, then click search button (magnifier icon).

User Group

Emergency

Facility Admin

Home User

Site

Editing Visitation Rules

To edit or delete a visitation rule, simply go to the Visitation Rules section of the Securus Video Visitation portal and click on the “edit” or “delete” button.

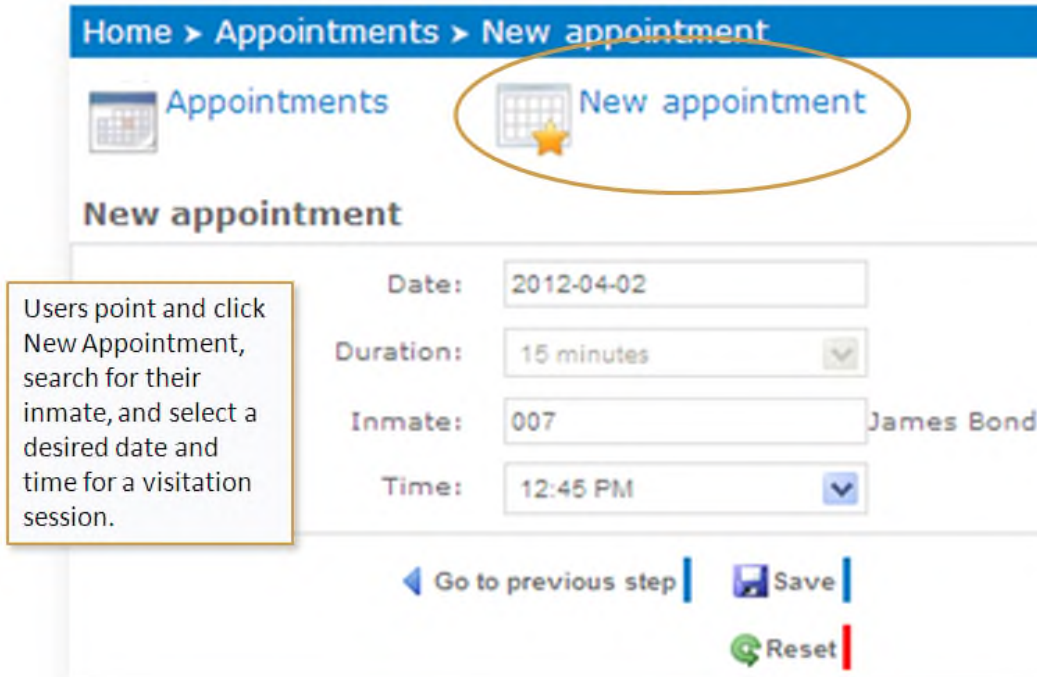
Editing Visitation Rules

Rule List								Actions
ID	Name	Visit Type	Quantity	Frequency	Start Date	End Date	Active	
176	Inmate 2 Visits per Week	Onsite	2	1 Week	2013-07-14	2020-12-31	<input checked="" type="checkbox"/>	<input type="button" value="edit"/> <input type="button" value="delete"/>
1 result								<input type="button" value="return to site"/> <input type="button" value="new"/>

User Account Set-up and Scheduling Features for Family and Friends Members

- Web-based and accessible from any standard web browser
- Simple user interface, enabling account setup and scheduling to be completed in minutes
- Automatically support multiple facilities in multiple locations with multiple housing units, making it easy to “find” the desired offender
- Automatically display only the visitation times and dates that are available
- Automatically send an email confirmation when a visit is scheduled, modified, or cancelled
- Allow users to easily change their personal information (password, address, phone number, etc.)

Secure Visitation Scheduling



Home > Appointments > New appointment

Appointments New appointment

New appointment

Date: 2012-04-02

Duration: 15 minutes

Inmate: 007 James Bond

Time: 12:45 PM

Go to previous step | Save | Reset

Users point and click New Appointment, search for their inmate, and select a desired date and time for a visitation session.

User Account Control and Scheduling Features for the Facility

- Secure, web-based access anytime/anywhere – providing different levels of authority and requiring unique usernames and passwords
- Point and click to view thorough user information including photo ID and easily approve or reject user account
- View, manage, report, and modify scheduled visits from the Securus Video Visitation dashboard
- Review historical staff usage through system user logs

The CenturyLink Team will work closely with the Department to implement established policies and procedures, including available visitation times, number of facility locations, number and location of each terminal, frequency of visits, registration approval requirements, check in procedures, time between visits, website naming conventions and other requirements.

25. **Proposer shall describe, in detail, their wireless containment plan that will restrict cellular signal, data, and text capabilities within a defined area around a Department facility. (Section C.3.1.1.W)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

As the Department is aware, Wireless Containment Systems (WCS) have evolved significantly over time and vary widely in their effectiveness. When CenturyLink installed the initial systems at McConnell and Stiles several years ago, WCS was a nascent technology evolving to cover LTE and new wireless protocols.

During the installation and testing phase, it became apparent that the prior system was not able to effectively evolve with technology. As a result, we worked with the Department to replace it with the current system...per TDCJ requirements and at our significant expense.

The new WCS solutions at both Units are up and running, covering all cellular protocols and passing the Department’s rigorous System Acceptance testing in compliance with the requirements of contract modification M-012. This solution has never failed formal System Acceptance testing, and is also deployed in the Florida and Georgia DOCs.

We believe our change of course on WCS is a prime example of our team’s commitment to TDCJ. When resolution is needed or new requirements emerge, we have worked with the Department to meet those needs.

WCS Architecture and Functionality

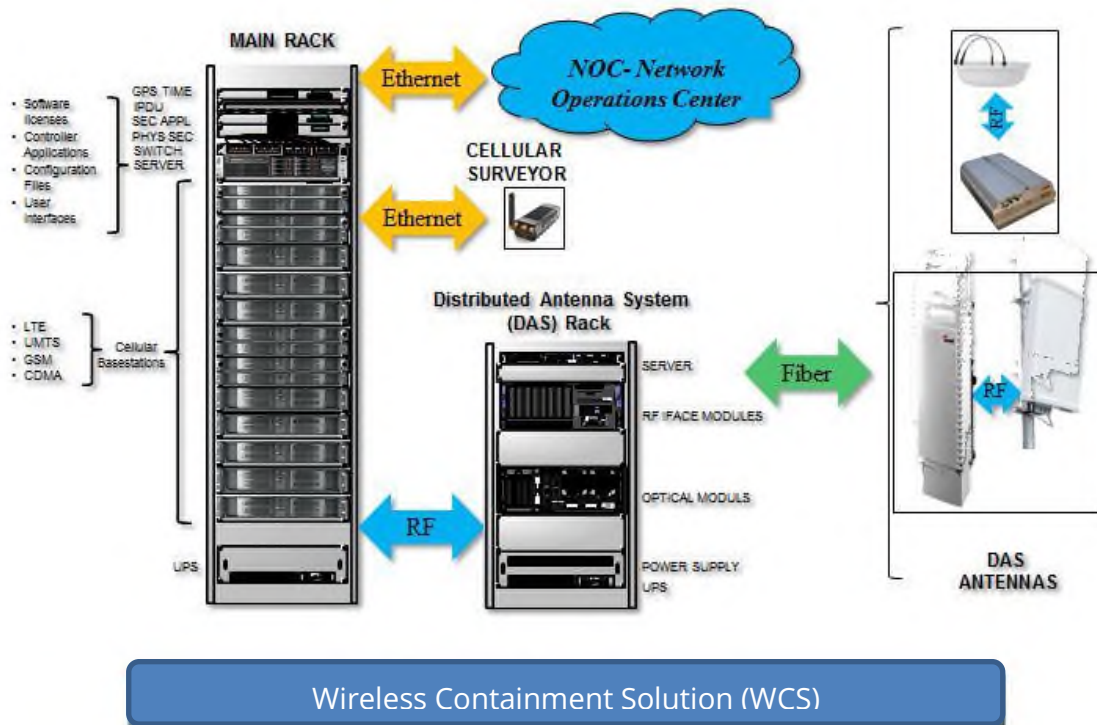
Under this new contract, we will continue to provide TDCJ a custom designed stand-alone turnkey private cellular telephone network and managed access system known as the Wireless Containment Solution (“WCS”) and services at the McConnell and Stiles Units.

The WCS service prevents unauthorized cell phone communications from being completed 24x7x365 days a year in the designated coverage areas of a controlled facility or prison.

SECURUS WIRELESS CONTAINMENT SOLUTION (WCS)



The WCS service includes data equipment racks that contain specialized radio controllers, base transceiver stations (“BTS”), proprietary software, radio frequency (“RF”) scanner, Global Positioning System (“GPS”), networking equipment, and uninterruptible power systems (“UPS”) as part of the service solution. The WCS also includes a distributed antenna system (“DAS”) which includes radio head-end interface units and remote optical units with antennas located throughout or around the Facility to provide the RF coverage for the Private prison cellular telephone network.



Wireless Containment Solution (WCS)

The WCS is currently operating to prevent unauthorized cell phone communications within the defined TDCJ coverage areas (“WCS Coverage Areas”).

The CenturyLink Team conducted comprehensive handset testing to identify high risk contraband cellphone use locations within the agreed upon coverage zones. System Acceptance Test results significantly exceeded performance standards set by the Department.

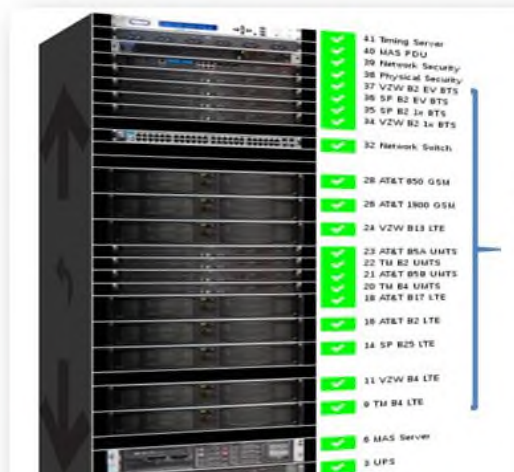
Operationally the WCS transmits signals to mimic or clone the commercial networks (example- AT&T, T-Mobile, Verizon and Sprint) as necessary to move all cell phones within the designated coverage areas of the facility from their commercial carriers respectively, to the Securus Private WCS cellular telephone network. Through the systems’ policy engines, it allows Authorized cell phones to communicate with an outbound call, and block or prevent all unauthorized cell phones from attempted calls, text/SMS, or data access, while also allowing all cell phones access to 911. This automatic process is provided 24 hours a day 7 days a week 365 days a year for the life of the contract.

The WCS will continue to provide the following services to TDCJ at each agreed facility deployed:

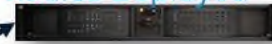
- a. Detect the operation of an illegally used cellular, mobile, or wireless device (a “Device”) within the offender housing units and other agreed to coverage areas at each facility.
- b. Log, record, and retain information for a Device when it is available (i.e., electronic serial numbers (“ESN”), International Mobile Subscriber Information (“IMSI”), and International Mobile Equipment Identifier (“IMEI”)) (the “Device Data”);

- c. Prevent Devices from accessing and therefore connecting to commercially available channels on mobile network operator networks to prevent completing a voice call, SMS/Text, or to access a data channel (access the general internet over a cellular data connection) in accordance with current laws and regulations.
- d. Send a customizable return text message to a Device attempting to send an SMS text, if desired by TDCJ.
- e. Allow outbound voice calls for agreed upon and authorized TDCJ cell phones (as detailed by specific TDCJ employee, by name, title, mobile phone TN – telephone number, IMSI, and IMEI) (the “Authorized Devices”), while preventing all other illegal, illicit, and/ or unauthorized communications, with the exception of emergency 911 access, all to 911 calls from any Device will be allowed to complete.
- f. Automatic monitoring and detection of WCS faults (state of Health) due to normal equipment or general component failure, and faults due to vandalism or tampering of systems, or attempts to disable system hardware or software, and provide alerts to agreed-upon TDCJ personnel regarding the same.
- g. WCS will not interfere with equipment operated by TDCJ within the designated WCS Coverage Area or the normal operation of cellular or wireless devices outside the WCS Coverage Area
- h. Subject to applicable laws and the parties’ mutual agreement regarding its use, make the Device Data available to authorized TDCJ users via a user interface (the “Device UI”)

The WCS is comprised of a both scalable and modular architecture and components. As technology changes, individual elements of the solution may be upgraded, including through the addition of base transceiver stations and DAS radio units and antennas as required.



Live Site Radios Deployed

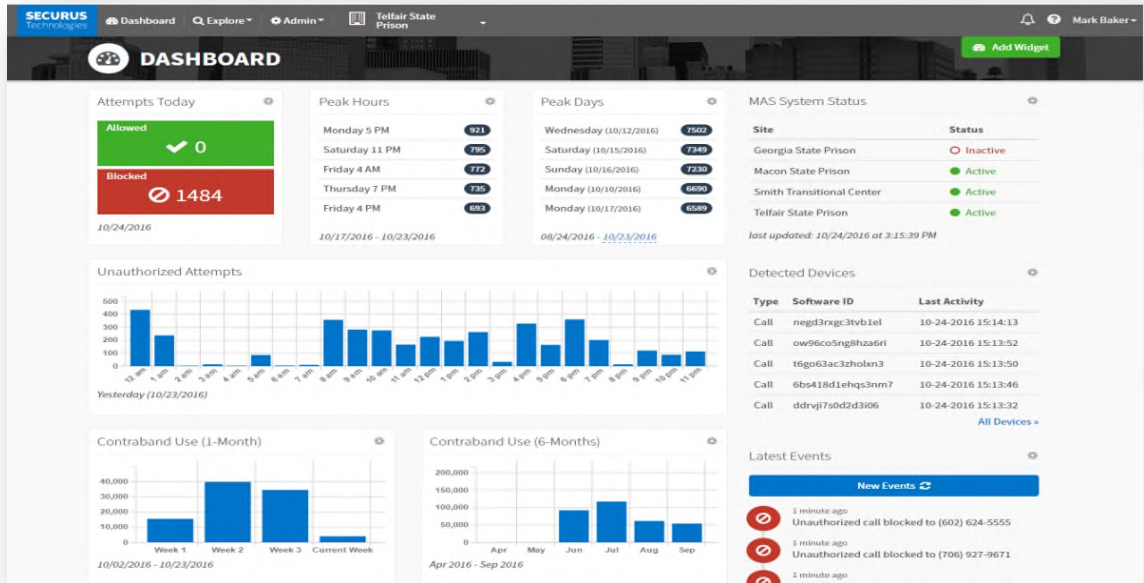


Securus’ DAS leverages a modular design that allows for new radio’s to be installed as protocols and technologies change.

As your partner, Securus will keep the system up to date throughout the length of the contract, installing radios as needed to address newly identified networks.

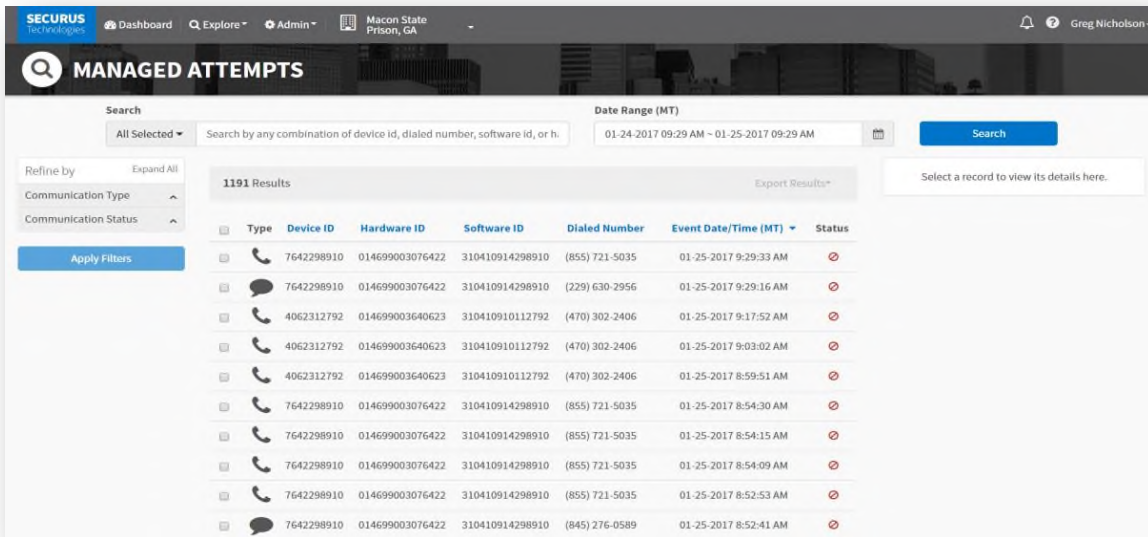
Training for TDCJ users is available at no cost at any time requested throughout the life of the contract.

Basic view and monitoring of the Systems through a web-based dashboard interface, including understanding of roles and permission based access security as implemented within the User Interface, Audit trail, and User management.



The management user interface provides system functions, including emergency shutdown procedures and Whitelist authorization and verification, report and audit queries, and exporting functionality in Excel, PDF or CSV.

TDCJ will continue to have access to manuals associated with the User interface software and its functions.



The CenturyLink Team will provide maintenance coverage for all System equipment, hardware components, servers and operating system software, radio controllers, base transceiver stations, radio units, antennas, sensors, networking equipment, power supplies and minor ancillary materials, and other monitoring elements, all that support the functionality of the Systems for so long as the Agreement is in force (“Maintenance Coverage”). Our Maintenance Coverage includes replacement by us of any part of the Systems that may require replacement due to normal operating conditions within the Unit environment and failure due to the normal use of the equipment where failure results. Consistent with our current WCS agreement, our Maintenance coverage does not include damage or equipment failure requiring replacement to the Systems that occurs as a result of the actions or conduct of TDCJ employees, agents, or offenders. Notwithstanding the above, we shall replace, at the cost and expense of TDCJ, any part of the Systems, including supporting components, that may become damaged or require replacement as a result of the actions or conduct of TDCJ employees, agents, or offenders.

In addition, we will provide a certified technician to perform all required Maintenance Coverage based on the following criteria:

- Priority 1 – Critical failure (also equivalent to a service failure where the Systems are considered inoperable) where 50% or more of the equipment in an entire facility or building is not functioning properly will be responded to remotely within 30 minutes; on-site arrival within 24 hours; resolution within 48 hours.
- Priority 2 – Major failure where less than 50% of the equipment in an entire facility or building is not functioning properly will be responded to remotely within 2 hours; on-site arrival within 48 hours; resolution within 72 hours.
- Priority 3 – Minor service issue or localized failure requiring repair, assistance, or maintenance will be responded to remotely within 4 hours; on-site arrival within 3 business days; resolution within 7 business days.

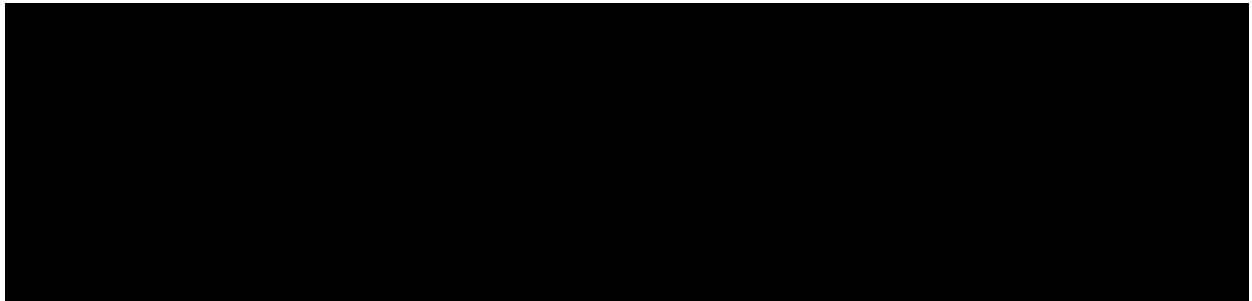
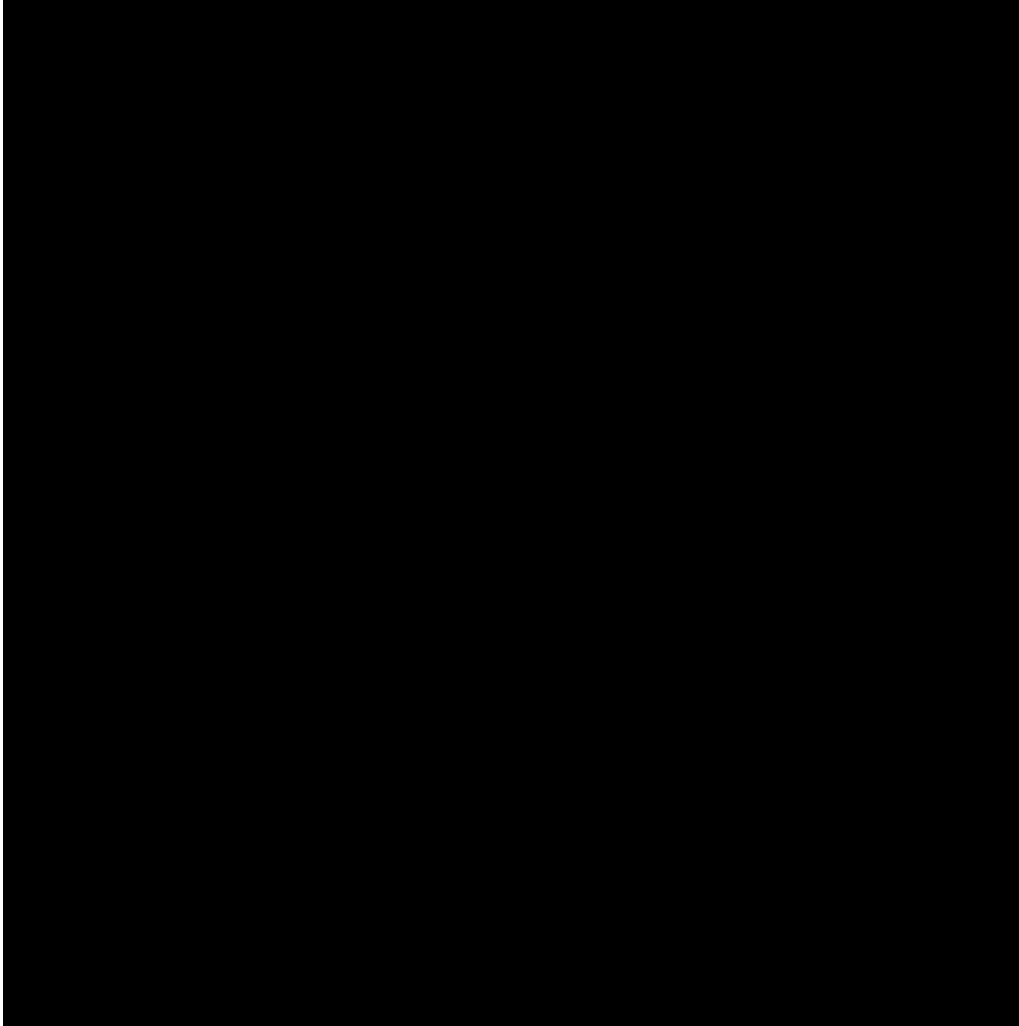
In addition, we will provide the necessary technicians and/or local field service staff, RF engineers and systems engineers to ensure optimal performance is sustained and that maintenance response and resolution time requirements are continually met. CenturyLink will develop and provide preventative maintenance plans and schedules, subject to approval by the TDCJ, during the life of the Agreement.

Remote monitoring will occur 7 day/24 hour/365 days through Securus’ Carrollton, TX based Network Operations Center (“NOC”) that is staffed by personnel to provide prompt resolution of any systems issues, problems, or fault events that occur at any time. The NOC and TDCJ Tech Support will serve as the primary point of contact for agreed upon and authorized TDCJ employees to report a maintenance or service issue or request.

26. Proposer shall provide FCC registration documentation. (Section C.3.1.2.A)

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The FCC Registration that will be implemented at the Department is as follows:



27. **Proposer shall detail by each designated site on the Site List (Exhibit J.1), the facility type being used to provide services, e.g. T1, Analog Central Office Truck, ISDN T1, etc. If the facility type used is the same for each designated site, a statement to that fact is sufficient. (Section C.3.1.2.B)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The CenturyLink Team will use Multi-Protocol Label Switching (MPLS) service (T-1's or N x T-1) at all facilities listed in Exhibit J.1 except for the Regional and Administrative Departments Monitoring Sites and for each of the four facilities listed below where other connectivity is used for VRS and WCS.

DSL Service:

- Regional and Administrative Monitoring Sites
- Murray - DSL for VRS and MPLS for OTS

Fiber-based internet over Ethernet:

- Estelle – Fiber-based internet over Ethernet for VRS and MPLS for OTS
- McConnell - Fiber-based internet over Ethernet for WCS and MPLS for OTS
- Stiles - Fiber-based internet over Ethernet for WCS and MPLS for OTS

Cable Modem

- OTS Management Office in Huntsville, TX

MPLS Service (T-1's or N x T-1)

- All other facilities

28. **Proposer shall explain how critical component redundancy will be accomplished, as well as state the length of time it takes for the system to reset. (Section C.3.1.2.C)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The infrastructure supporting the OTS was built for high availability and full redundancy. Each device (routers, switches, servers, SAN, power, circuits, etc.) within the infrastructure is both fault-tolerant (down to the component level) and physically redundant with automatic fail-over. Our routers and servers have dual CPUs, NICs, power supplies, and A & B power feeds. The telecommunications circuits provided by our service providers for network access are both redundant and diverse.

While operating on a single platform, 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

Only the CenturyLink Team can provide two redundancy tests every year on the TDCJ SCP system. This service is performed exclusively for TDCJ to provide backup assurances, and is something no other vendor has the resources to perform.

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 offender 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 define stringent service level agreements in the event of failure.

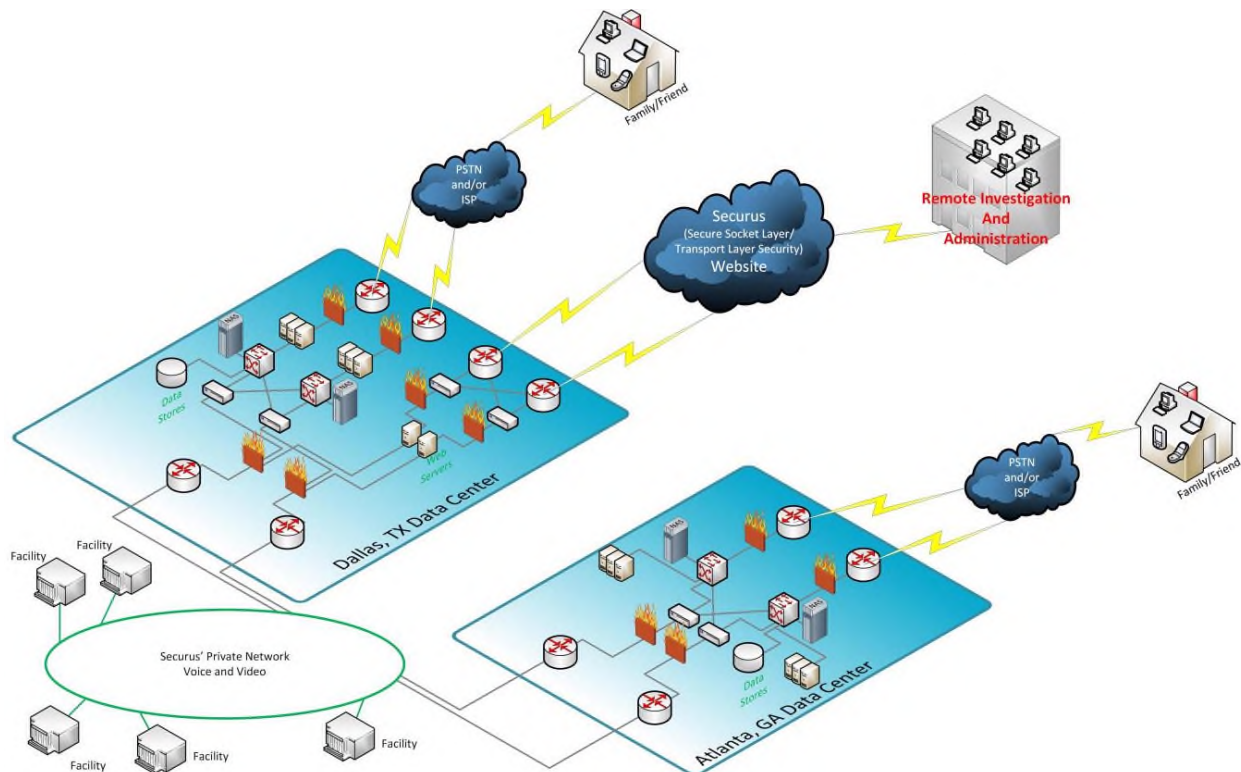
In the event of a temporary local outage of commercial power at the facility, an Uninterruptible Power Supply (UPS) is provided as a redundant back up to continue operation of all equipment installed on-site. The UPS is self-charged, and the equipment self-initializes without manual intervention when commercial power is restored.

Additionally, each of our data centers has an uninterruptible power supply (UPS), and a generator to provide maximum network uptime. The traditional data circuits (MPLS, Frame Relay, VoIP) all have dual connectivity feeds to/from the telecommunication carrier to each of our data centers.

Summary of Redundancy and Security	
OTS Redundancy on Multiple Levels:	<ul style="list-style-type: none"> ✓ Hosted in Class IV Data Centers ✓ Multiple power grids ✓ Redundant transport carriers (in and out of the data centers) ✓ Multiple building entry points for power and transport
Data Center	<ul style="list-style-type: none"> ✓ Data Center locations in different states (Texas and Georgia) ✓ Minimum of two diverse paths into each data center ✓ Redundant fault tolerant enterprise grade components ✓ Servers are clustered with load balancers to manage the load applied to each server <ul style="list-style-type: none"> ○ If one server goes offline or load is at a max threshold, requests go to the next available server. ✓ Redundant HVAC ✓ Full access audit with biometric controlled security

Data Redundancy	<ul style="list-style-type: none"> ✓ Each data center supports RAID storage configurations ✓ Recordings stored in multiple locations: Primary and Secondary <ul style="list-style-type: none"> ○ Calls are initially recorded on primary recording servers ○ Secondary servers – within 15 seconds of the call completion, calls are moved from the recording servers to the secondary servers. ✓ Databases and call recording storage constantly synchronized
Onsite	<ul style="list-style-type: none"> ✓ Uninterruptible Power Supply (UPS)
Network	<ul style="list-style-type: none"> ✓ Separate transport & termination carriers ✓ Instantaneous carrier failover ✓ Multiple network switches which fail over to each other (A & B side) ✓ Multiple network routers which fail over to each other (A & B side) ✓ All devices (hardware) have multiple power supplies connected to AC Power (A & B side power) ✓ Outages automatically diagnosed from remote NOC

Co-Located Secure Connect Network



29. Proposer shall submit an equipment room layout including all equipment to be installed during the project. (Section C3.1.2.D)

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

As the OTS is a centralized, network based solution, limited amounts of equipment are placed within the physical equipment room at each Department facility location. The CenturyLink Team works with the Department to make sure that the equipment that resides at a TDCJ facility does not interfere with the Department's access, use, or potential use of the equipment room.

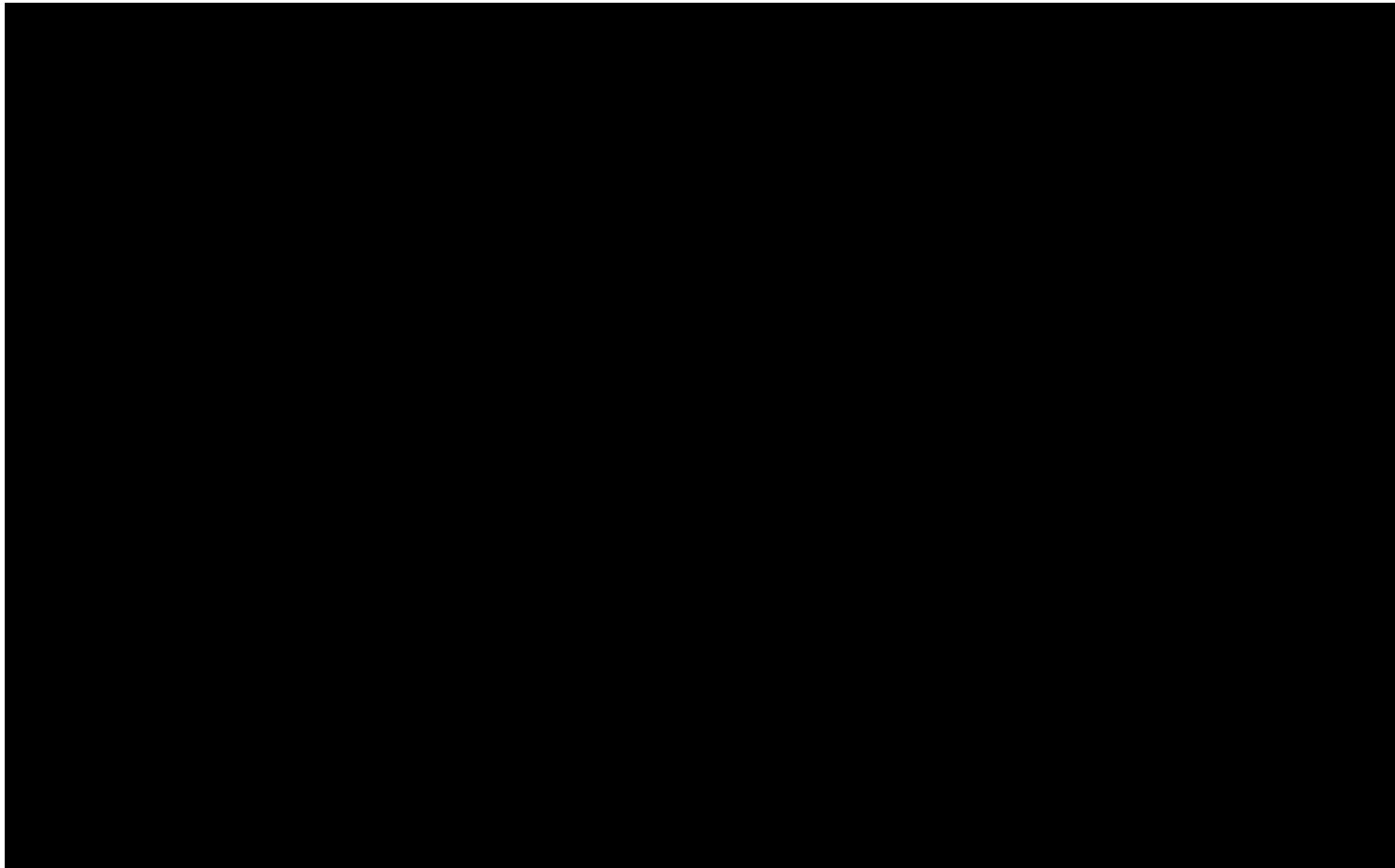
Each indoor node cabinet will contain the following items:

- ADTRAN Total Access Series Integrated Access Device (IAD): The Total Access 900 Series offers a T1 network interface and includes up to 24 FXS ports for connection to offender phones, an integrated DSX-1 port, and a 10/100 Base-T Ethernet interface for access to the MPLS (Multi-Protocol Label Switching) network.
- NETVANTA: The NetVanta 1234 is a fully managed Layer 2 Ethernet switch designed for cost-effective Ethernet switching. This scalable, full-featured product is suitable for networks requiring Layer 2 switching for interconnecting LAN devices or network segmentation.
- BULKHEAD Patch and Splice: All Telect bulkhead panels for splicing.
- CORNING SPLICE TRAY: Corning Cable Systems Fiber Splice trays for fiber organization technology to provide optimum physical protection, management, and bending radius for spliced fibers.
- 4KSU with MLLT1/MDS 25/ITE modules: The 4KSU provides ground for the Adtrans and the MLLT1 protects the MPLS and the MDS 25 protects the Adtran station cards when they are extended out of the building where the node resides; as do the ITE protective modules.
- APC UPS 450 or Eaton Powerware 5115 1000W RM UPS.

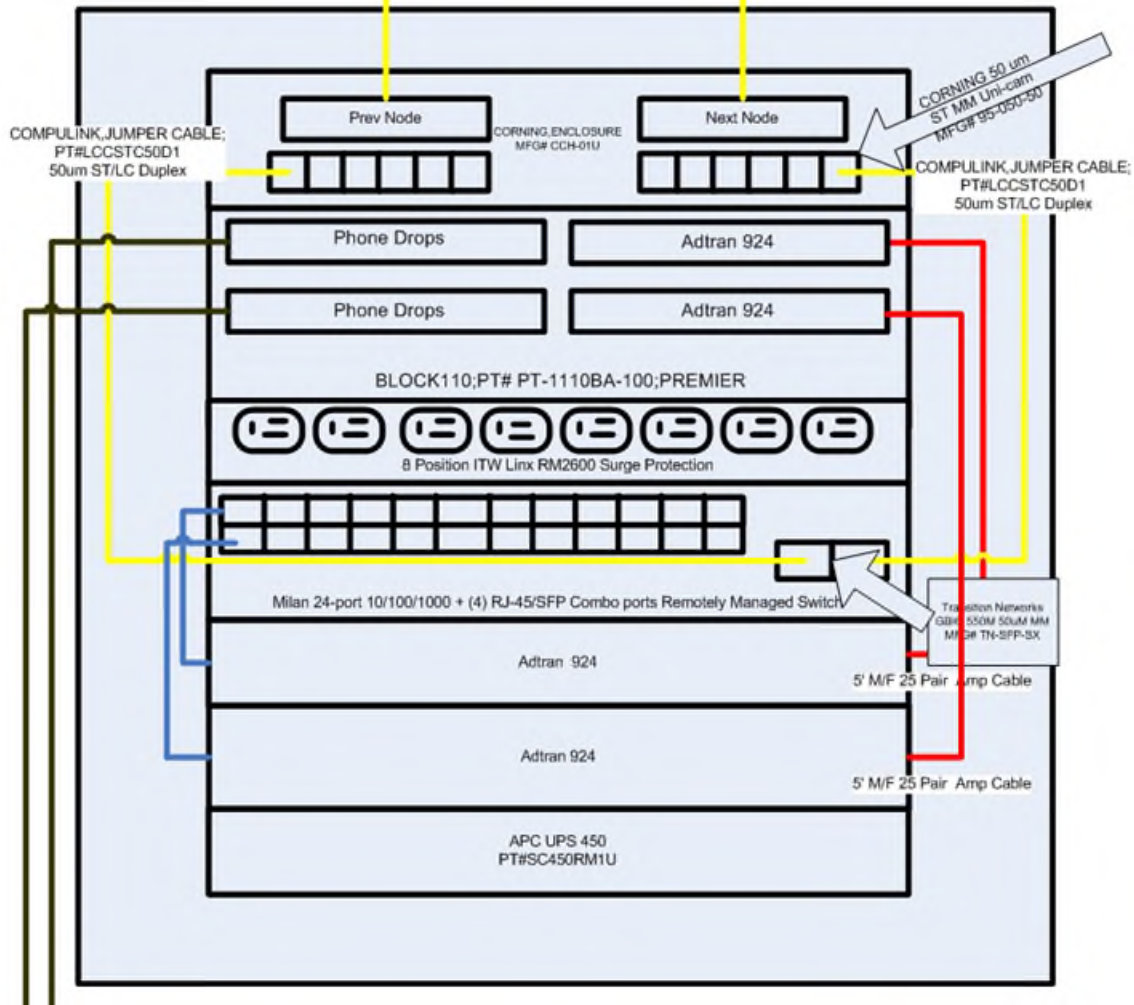
The equipment will be installed in a secure indoor **American Products Ventilated Cabinet MFG # SEC-322325 approve by and built specifically for Texas Department of Criminal Justice** at each location. You will find the specification sheets for TDCJ Node Cabinet on the following pages.







Example of Equipment Inside of Node Cabinet



As the current provider, we are experienced with the space limitations of TDCJ equipment rooms. We have installed all required equipment within these designated rooms without the need of constructing addition equipment buildings. Although we do not anticipate needing additional separate equipment rooms at any TDCJ location, we do have the capability to do so if need be.

Any equipment that will be installed outdoor will be installed in a secure outdoor cabinet at each location that is fully compliant with the Department's requirements.

Examples of the CenturyLink Team's Installations at TDCJ Facilities



30. Proposer shall describe or provide descriptive literature on the Offender telephones. (Section C.3.1.2.E)

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

Our offender telephones are the strongest and most reliable units available and are designed specifically for the prison environment. These phones are the overwhelming choice for state prison systems, the Federal Bureau of Prisons, county, and city facilities nationwide because of their proven reliability, durability, and flexibility. All Offender telephones are:

- Compatible with the mutually agreed on biometric caller identity verification system
- Wall mounted or pedestal
- Stainless steel
- Tamper-resistant (anti-vandal and anti-drill)
- Of durable construction
- Flame retardant and do not give off toxic gases when subjected to fire
- DTMF compatible
- Labeled on the body per Department requirements

- FCC and Underwriters Laboratories (UL) approved with certification number
- Compatible with TDD devices and meet all ADA requirements.
- Equipped with hearing aid compatible handsets
- Equipped with cords from the receiver to the body of the telephone that is approximately two (2) feet and armored. *different cord lengths can be provided at the Department's request

CenturyLink Public Communications, Inc.
This call is subject to being monitored and recorded.

Press '1' for English.	Enter area code and phone number.
Marque '2' para Español.	Marque su numero de telefono, incluya su codigo local o lada.
For a collect call press '1'.	Say your full name to verify your voice.
Para llamada a cobarse, marque '1'.	Diga su nombre completo para verificar su voz.
For a debit call press '2'.	You may hear silence during the acceptance of your call. Please continue to hold.
Para llamada por débito, marque '2'.	Vas a oír silencio mientras aceptan su llamada.
Enter your PIN Number.	Continue esperando por favor.
Marque su numero de identificación personal.	

Below please find detailed specification on the telephones.

The CenturyLink Team is proposing the Wintel Model 7010 Series telephone due to its durability and reliability. In addition, Wintel's "confidencer" filters out background noise, allowing for better sound quality for verification of offender's voice print, improved sound quality to the called party, and higher quality call recordings.

ITC7010 Mini Coinless Telephone with Volume Control

DIMENSIONS: 11-1/2"Hx 5"W x 2-1/2"D

WEIGHT: 7.1 lbs

Features/Options

The proposed phone models include the following features:

- Built-in user controlled volume "LOUD" button for ADA-mandated volume control (user must have control of volume amplification, AND volume must reset to normal with hang up to meet ADA requirements)
- Cold rolled steel provides rugged vandal resistant telephone housing designed for offender use



- Confidencer technology, built into every dial, filters out background noise at the user's location, allowing better sound to the called party
- All-in-one electronic dial features modular incoming line and handset connections for quick maintenance. Carbon (HS) and DuraClear® (DURA) Handsets have separate 4-pin connections.
- Heavy chrome metal keypad bezel, buttons, and hook switch lever withstand abuse and vandalism
- Armored handset cord is equipped with a steel lanyard (1000-pound pull strength) and secured with a 14-gauge retainer bracket for maximum vandal resistance
- Handset has sealed transmitter and receiver caps, suitable for heavy use and abuse locations
- Pin-in-head security screws minimize tampering
- Hearing aid compatible and FCC registered US: 1DATE05BITC-254, IC: 3267A-ITC254

Superprint 4425 by Ultratec

The phone offers the most advanced printing TTY with 32 K memory, including:

- Built-in 24-character printer
- Three selectable print sizes
- Keyboard
- Call progress (display shows whether line is ringing or busy in direct connect)
- Tone dial
- Auto ID
 - Turbo code
 - Time and date
 - TTY voice announcer
 - User-programmable relay voice announcer
 - 20-character vacuum fluorescent display
 - Rechargeable batteries
 - Optional ASCII code
 - Optional large visual display port (includes ASCII)



sPhone XL™

The Securus sPhoneXL terminal is a correctional-facility grade, tamper-proof steel enclosure. The hardware is wall mounted unit equipped with a built-in shatter resistant touch screen, a high-resolution video camera with integrated lighting, and tamper-proof, heavy molded plastic handset with an armor-reinforced cord for audio communication, and surge protection.

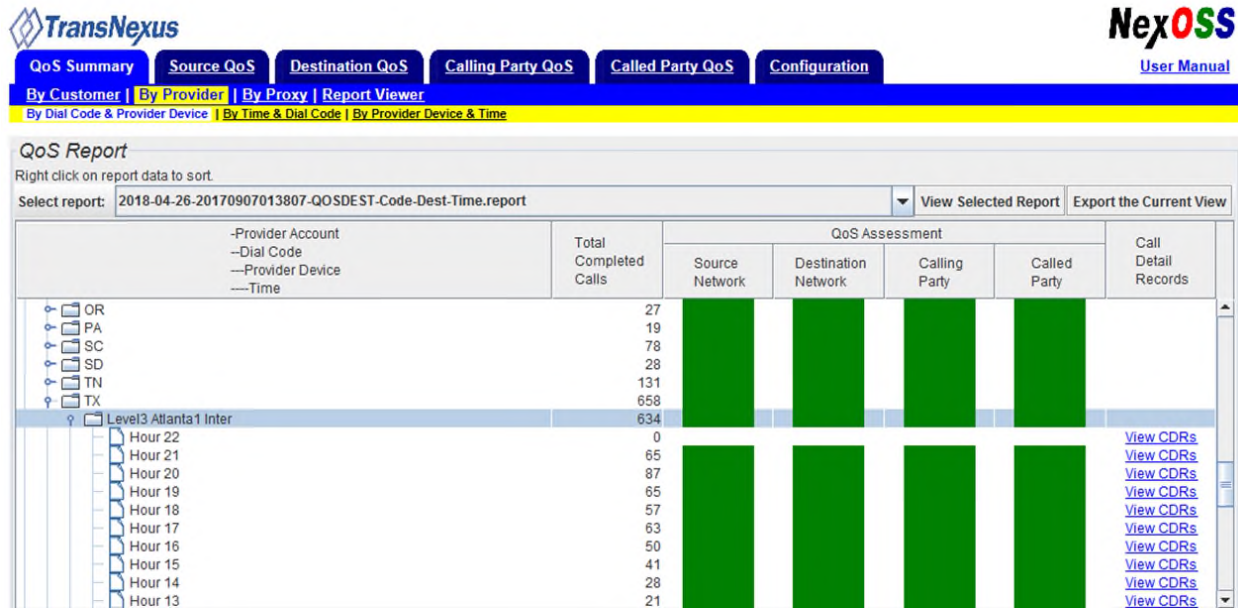


- Light and ruggedized vandal-proof terminals (hardened steel): Best balance between weight and resistance
- Sealed: Dust and
- Liquids Resistant, spill-proof (accidental or deliberate).
- Assembly elements are hidden: No screws or hinges can be removed and used to manufacture weapons. No doors/compartments that can be opened in the front or on the sides of the unit.
- Rounded edges that reduce the risks of accidental or intentional injuries.
- Abrasion and chemical resistant; the unit can be cleaned using commercial cleaning agents.
- Humidity and corrosion resistant
- Built-in LCD 15" with hardened shatter resistant touch screen
- HD camera, autofocus, (720p @ 30 fps)
- Sphone XL PoE has movable camera with a 2MP (1600x1200) resolution
- Optional hands free terminal with built-in HD video camera, Pan-Tilt-Zoom, 10x optical zoom, 4x digital zoom, 30fps
- Built-in LED lighting system
- Power ON LED indicator
- Magnetically activated pushbutton for on/off power
- Built-in heat sink mounted to the back for heat dissipation
- Built-in protection device against voltage variations
- Vandal-proof handset. Armored cable
- Standard non-proprietary computer components
- All electrical components comply with UL, CE and/ or CSA
- System maintenance via wireless keyboard (Infra Red Access)
- Mother board: Micro/Mini ATX
- Intel Quad Core 2 GHz processor
- Memory: DDR3; RAM 4,096 MB (4 GB)
- Solid State (SSD) Hard drives to reducing moving components and potential failure points. • Network: Ethernet RJ-45 (CAT5/6)
- Power Options:
 - AC: 110V 2 amps
 - Low voltage DC: 24 V 8.33 amps
 - Power over Ethernet: IEEE802.3at (PoE Plus).

31. Proposer shall explain how Quality of Service for voice prioritized packets will be accomplished. (Section C.3.1.2 .F)

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

Call Quality is measured by Mean Opinion Score (MOS) in a range of 1 through 5; One being the lowest score and 5 being the highest. Securus uses IP packet tagging, based on the type of device connected to the network, to enable the prioritization of voice packets over data packets, maintaining a MOS rating of 3.7 or better. This prioritization is honored within the Securus network devices starting at the customer facility, and continues as well to the Securus data center network, in order to maintain the desired Quality of Service (QoS). Securus uses call statistic records from its Session Border Controllers to calculate a Mean Opinion Score (MOS) on each call and regularly reviews summaries of that data to confirm QoS levels are maintained above required standards. Please see example below.



The screenshot shows the TransNexus QoS Report interface. At the top, there are navigation tabs: QoS Summary, Source QoS, Destination QoS, Calling Party QoS, Called Party QoS, and Configuration. A 'User Manual' link is also present. Below the tabs, there are filters for 'By Customer', 'By Provider', 'By Proxy', and 'Report Viewer'. A yellow bar contains filters for 'By Dial Code & Provider Device', 'By Time & Dial Code', and 'By Provider Device & Time'. The main report area is titled 'QoS Report' and includes a 'Select report:' dropdown set to '2018-04-26-20170907013807-QOSDEST-Code-Dest-Time.report'. Below this is a table with columns for Provider Account, Dial Code, Provider Device, Time, Total Completed Calls, QoS Assessment (Source Network, Destination Network, Calling Party, Called Party), and Call Detail Records. The table shows data for various states (OR, PA, SC, SD, TN, TX) and a detailed view for 'Level3 Atlanta1 Inter' with hourly breakdowns. All QoS Assessment cells are green, indicating good performance. 'View CDRs' links are provided for each row.

-Provider Account --Dial Code ---Provider Device ---Time	Total Completed Calls	QoS Assessment				Call Detail Records
		Source Network	Destination Network	Calling Party	Called Party	
OR	27	Green	Green	Green	Green	
PA	19	Green	Green	Green	Green	
SC	78	Green	Green	Green	Green	
SD	28	Green	Green	Green	Green	
TN	131	Green	Green	Green	Green	
TX	658	Green	Green	Green	Green	
Level3 Atlanta1 Inter	634	Green	Green	Green	Green	
Hour 22	0	Green	Green	Green	Green	View CDRs
Hour 21	65	Green	Green	Green	Green	View CDRs
Hour 20	87	Green	Green	Green	Green	View CDRs
Hour 19	65	Green	Green	Green	Green	View CDRs
Hour 18	57	Green	Green	Green	Green	View CDRs
Hour 17	63	Green	Green	Green	Green	View CDRs
Hour 16	50	Green	Green	Green	Green	View CDRs
Hour 15	41	Green	Green	Green	Green	View CDRs
Hour 14	28	Green	Green	Green	Green	View CDRs
Hour 13	21	Green	Green	Green	Green	View CDRs

32. Proposer shall describe, in detail, staffing functional requirements, as well as copies of appropriate licenses and certifications. (Section C.3.2.2)

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The CenturyLink Team exceeds the Department’s staffing requirements. We have dedicated qualified staff solely to perform the services required to the TDCJ, both out in the field and at headquarters. We have created specific TDCJ teams to facilitate account registration and technical support. All CenturyLink Team members providing services are qualified, appropriately trained and certified when necessary, to ensure knowledge levels in excess of the Department’s expectations.

The CenturyLink Team has worked very hard to develop a good working relationship with the Department staff and other contractors working with the Department in order to facilitate easy coordination and communication.

All of the personnel that the CenturyLink Team has dedicated to TDCJ have passed the Department required background clearance and any future new personnel will be subject to the same standards. Additionally, as the personnel on our dedicated TDCJ account team have already been trained and been working on providing service to the Department, they are well versed in the procedures and standards of conduct prescribed by law, and as prescribed in the Department's personnel policy and procedure guidelines, particularly the rules of conduct, employee uniform and clothing requirements (as applicable), security procedures, and any other applicable rules, regulations, policies and procedures of the Department. The CenturyLink Team's staff will be subject to and will comply with all security regulations and procedures of the Department and the respective facility. We understand that violation of regulations may result in the employee or individual being denied access to the facility. In this event, the CenturyLink Team will provide alternate personnel to supply services described herein, subject to Department approval.

The CenturyLink Team will utilize only qualified personnel for the services and support required by the Department. The Department will be provided prior written notice of placement and/or replacement of personnel, or any plan to place and/or replace personnel prior to any changes of staff being made.

All personnel assigned to the support of the Department will be fully briefed on all laws, rules, regulations, standards, policies and procedures by the CenturyLink Team to ensure complete compliance with this requirement. The CenturyLink Team will provide criminal history information and information for employee background checks.

Not only does the CenturyLink Team meet the staffing requirements, we exceed expectations currently and will continue with the new contract. Following are descriptions of the functional responsibilities associated with the CenturyLink Team staffing positions:

Position Title	Job Description
Account Manager-Primary	<p>The CenturyLink Team already has assigned a full time Account Manager, our equivalent to a Customer Service Manager, which will continue to be exclusively dedicated to the TDCJ for the full term of the agreement. He serves as the primary point of contact for the Department. The duties of the Account Manager include, at a minimum:</p> <ul style="list-style-type: none"> ▪ Overall responsibility for performance of the OTS ▪ Customer advocate to CenturyLink Team management ▪ Commissioning and billing resolution ▪ Service and technical issue resolution ▪ Training, attendance at on-site meetings ▪ Promptly responding to Department and offender family requests, which shall include, but not be limited to e-mail, telephone and facsimile requests.

Position Title	Job Description
Account Manager-Alternate	Additionally, the CenturyLink Team already has assigned a full time Alternate Account Manager that will continue to be solely dedicated to TDCJ for the full term of the agreement. She works in coordination with the other Account Manager to fulfill all of the responsibilities listed above.
Service Representative and Data Administrator Manager	<ul style="list-style-type: none"> ▪ Responsible for installing, maintaining, and supporting the OTS system and additional products and service used by TDCJ ▪ Manage, hire and train all support personnel teams that provide customer service and technical support to TDCJ facility staff, as well as offenders and Friends and Family customers ▪ Promptly responding to Department when escalations occur ▪ Attendance at Department meetings when necessary ▪ Supports training initiatives for TDCJ personnel
Service Representative and Data Administrator Supervisor	<ul style="list-style-type: none"> ▪ Supports efforts to hire, train, and schedule all support personnel teams that provide customer service and technical support to TDCJ facility staff, as well as offenders and Friends and Family customers. ▪ Provides Level 3 escalation support.
Dispatcher	<ul style="list-style-type: none"> ▪ Manages all Field Technician dispatches for service issues and supervised PBI enrollments. ▪ Manages all TDCJ mailroom E-messaging/kite printing consumables ordering/deliver (paper, printer toner, drums, etc.)
Service Representatives	<p>The CenturyLink Team has eighteen full time Service Representatives dedicated to the contract for the successful implementation of the project and ongoing support of the OTS. The Service Representatives shall maintain a high level of ongoing effective communication with Department staff to assure quality customer service is being provided to all customers and issues are being resolved in a timely manner. Service Representatives will be directly responsible for:</p> <ul style="list-style-type: none"> ▪ General Customer Service to the Department ▪ Help Desk for Administrative support ▪ Data entry input - data integrity ▪ Intake Center enrollment/training of new offender's (field Service Reps) ▪ Updates to PIN, PAN, PBI enrollment (central Service Reps) ▪ Follow-up with the facility to insure all systems are

	<p>operational and work is completed thoroughly and accurately</p> <ul style="list-style-type: none"> ▪ Administrative support of prepaid transactions ▪ Investigation of offender and staff complaints, processing of internal documents, and generating reports as requested ▪ Keeping accurate logs and documentation conveying messages and information in writing and/or via e-mail ▪ Advise management and open tracking tickets for all facility service affecting issues ▪ Help with effective operation of OTS components including hardware, software, and telephony equipment (when necessary).
<p>Data Administrators</p>	<p>The CenturyLink Team has six full time Data Administrators (Technical Help Desk Representatives) dedicated to the contract for the successful implementation of the project and ongoing support of the OTS. The Data Administrators will be directly responsible for:</p> <ul style="list-style-type: none"> ▪ Detailed troubleshooting/problem resolution as well as root cause analysis for all new and escalated tickets ▪ Responsible for accepting and/or assisting in problem analysis for Level 1 escalation ▪ Status customers on open issues and provide ETA of resolution ▪ Accurately document trouble tickets including root cause, problem analysis resolved and steps to final resolution ▪ Ensure resolution is verified with customer for all tickets before closure ▪ Work with Field Technicians to fully resolve problems ▪ Proactively maintain and scrub every system each time a troubleshooting event occurs ▪ Answer incoming customer and field technician calls • Ability to perform all functions of Level 1 Technician • Participation of on call rotation ▪ Work projects as necessary ▪ Provide mentoring to Level 1 technicians ▪ Perform other duties as needed which are dictated by the business needs of the service organization and assigned by management

Position Title	Job Description
Field Repair Site Technician Manager	<p>The CenturyLink Team has a full time Field Service Manager dedicated to the contract for the successful implementation of the project and ongoing support of the OTS. The appointed Field Service Manager is directly responsible for:</p> <ul style="list-style-type: none"> ▪ • Supervision of fifteen Field Repair Technicians ▪ Oversee repair and maintenance ▪ Oversee initial PBI enrollment ▪ Customer advocate to CENTURYLINK Team management ▪ Attendance at Department meetings when necessary ▪ Promptly responding to Department when escalations occur
Field Repair Site Technicians	<p>The CenturyLink Team has fifteen full time Field Service Technicians dedicated to the contract for the successful implementation of the project and ongoing support of the OTS. Field Technicians are directly responsible for:</p> <ul style="list-style-type: none"> ▪ Field Services Technicians (FST) are required to maintain, repair and operate telecommunications hardware, LAN/WAN/Networking hardware/ software, various electronic equipment and wiring per specifications and operational procedures at correctional facilities nationwide. ▪ Installing, maintaining, programming and repairing telecommunications hardware, associated LAN/WAN/Networking hardware/software, various electronic equipment and wiring per specifications and operational procedures. ▪ Working in a one-on-one basis with sworn facility staff, civilian facility staff, the offender population and the family members of offender's to resolve questions and concerns regarding billing, training, technical support and operational issues. ▪ Monitors and tests equipment according to published equipment standards. ▪ Interface with all internal CenturyLink Team organizations, various vendors and contractors for problem solutions. ▪ Assess and respond to situations where standard procedures have failed in isolating or resolving problems. ▪ Required to complete TIA A+ Certification, as well as, a minimum of 2 years experience working with Cisco based routers, switches and PIX firewalls.

Position Title	Job Description
Enrollment Center Manager	<p>The CenturyLink Team has an Enrollment Center Manager already in place to continue service under this new contract. The Manager serves as an important point of contact for the Department for consumer service and security topics. The duties of the Manager include:</p> <ul style="list-style-type: none"> ▪ Overall responsibility for performance of the Enrollment Center ▪ Ensure all approved enrollments meet Department guidelines ▪ Manage Attorney Registration and Audit Process ▪ Manage Enrollment Center Representatives with progressive levels of responsibility to ensure all levels of support to the Department and offender Families are provided. ▪ Manage Offender Debit Refund Process. ▪ Promptly respond to escalations and requests from the Department, Attorneys, and offender families received by phone, email & facsimile. ▪ Interface with consumer billing service center management to coordinate approvals and consumer account management.
Enrollment Center Supervisors and representatives	<p>The CenturyLink Team has existing full time Verification Representatives (currently 16) dedicated to the contract for the successful implementation of the friends and family enrollment project and ongoing support of the OTS. The Verification Representatives maintain a high level of ongoing customer service to all customers and ensure enrollments are processed in a timely manner. The primary duties of the Verification Representatives are:</p> <ul style="list-style-type: none"> ▪ Process each friend or family enrollment request received using the following methods: phone, fax, email or U.S. Mail. ▪ Troubleshoot and direct customers for quick and accurate resolution. ▪ Input customer account data and perform audits to ensure data integrity. ▪ Process Attorney registrations and conduct quarterly Attorney Audits Data to ensure data integrity. ▪ Process offender debit refund requests. ▪ Respond to email inquiries from offender families and the Department in a timely manner. ▪ Manually update the Department's daily block report

Position Title	Job Description
Digital Forensic Lab Staff	<p>The CenturyLink Team has a Cellular Forensics Laboratory; co-located with the Office of Inspector General (OIG) in Austin, TX, dedicate to TDCJ. The lab is currently staffed with 3 forensic examiners whose primary duties are:</p> <ul style="list-style-type: none"> ▪ Data extraction from recovered contraband cell phones ▪ Ad-hoc reporting of data extracted from contraband cell phones
Call Monitoring Staff (GEX) – TBD	<p>Guarded Exchange analysts are directly responsible for providing TDCJ investigative support by:</p> <ul style="list-style-type: none"> ▪ Call monitoring using investigative software with the purpose of identifying actionable leads ▪ Preparing reports based on their analysis
Trainers	<p>The CenturyLink Team has a dedicated training department that will provide all necessary training to Department Staff.</p> <p>Additionally, the Account Managers and the Technical Support Manager will be responsible to for fulfilling the Department’s training. As they are members of the staff dedicated to the day to day of TDCJ, they are best equipped to train Department Staff on their own data.</p> <p>The same core system will be used if we are awarded the new contract, eliminating the need for extensive re-training.</p> <p>The Training Department is directly responsible for:</p> <ul style="list-style-type: none"> ▪ Delivery of product training programs using a variety of training tools ▪ Conducting on-site customer training sessions ▪ Aligning product training to meet customer needs and expectations ▪ Defining content for training presentation materials ▪ Implementing standards and guidelines for customer product training ▪ Developing standardized customer training materials (instructors guides, training outlines and training syllabus) ▪ Delivery product Webinars ▪ Increase the Department's understanding and utilization of OTS ▪ Assess customer satisfaction with trainer and training

Additional Staffing for Implementation Process

Implementation Manager

Paula Parson will be the Implementation Manager dedicated to this project full-time. Her Implementation Manager responsibilities include:

- Manage team of Installation Technicians
- Manage software installations
- Manage installation process of OTS specific electronics in cabinet, phones, workstations, printers and any other ancillary systems from beginning to end
- Work with management and technicians to set project objectives, priorities and deliverables
- Ensure successful execution of all installation programs, including video visitation
- Manage the customer delivery and follow correct policies and procedures in the building of our equipment - management of all outsourcing activities
- Ensure all programming, connectivity and configurations meet company standards
- Schedule resources for meeting project deadlines

Certifications

The CenturyLink Team currently employs 17 dedicated field technicians assigned to TDCJ with a combined average of 6.8 years of experience successfully servicing the Texas Department of Criminal Justice OTS. Many of whom have serviced the OTS from inception to present.

We ensure that every technician is technically proficient with equipment and methods, familiar with the rules and regulations of the facility, and committed to delivering outstanding customer service performed in a specified manner.

CenturyLink technicians currently assigned to TDCJ support hold numerous certifications that include:

CompTIA

- CompTIA A+ ce
- ComptTIA N+ ce
- CompTIA Security+ ce
- CompTIA Cloud+ ce
- 4 CompTIA Stack Certs
- CompTIA Network+ Certified

SNIA Education Certifications

- Solid State Storage
- Strategies & Technologies for Data Protection
- Storage Implications in Virtualization
- Innovations in Data Management & Disaster Recovery
- Architecting & Implementing a Fiber Channel SAN
- Active Archive

Dell Certifications

- 577 Basic Wireless Technology – Certification
- 722 Trusted Advisor for Field Service
- 530 DSP Televisions - 4200 Plasma TV
- 836 Workstations - Precision R5400 - Certification
- 644 DSP Televisions - TV 101 Certification
- 523 Dell ESD - Certification
- 884 Portables - Vostro A840 Acknowledgement
- 787 Desktops - ATX V.1 Certification
- 792 Portables - Latitude D630 XFR - Certification
- 873 Portables - Latitude E6400, E5400, E6400 ATG, Precision M2400 - Certification
- 874 Portables - Latitude E6500, E5500, Precision M4400 – Certification
- 815 Portables - Vostro 1510 - Certification
- 814 Portables - Vostro 1310 - Certification
- 802 Customer Handling Skills Certification
- 783 Foundation 2008 Desktop
- 781 Foundation 2008 Portables
- 709 DSP Client – On-Site Troubleshooting w/Power Tester Certification

Other Certifications

- Codes Standards and Communications Cabling Certification
- Vantage Advanced Q-Series Products Certification
- Fiber Optic Training Certificate
- Avaya Certification
- Journeyman Electrician
- 2017 Stevie Gold Winner

Our team is required to take on-going annual courses in order to stay up to date with changes in the industry. Our technicians are also required to spend a designated amount of time each month practicing equipment updates and change outs in order to minimize service outage intervals on trouble calls.

33. Proposer shall identify a dedicated full-time Project Manager. (Section C.3.2.2.A)

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

Paula Parson will be the Project Manager dedicated to this project full-time. She will be in charge of the implementation project team and be the point-of-contact through implementation, acceptance, and go-live. She will be in regular contact with Department personnel via phone calls, emails, and in-person visits. Once implementation is completed, she will return to her roles as Co-Account Manager.

As the project manager she will be responsible for:

- Supervising all teams that make up the TDCJ Implementation Project Team.
- Evaluating and distributing resource allocation
- Coordinating equipment deliveries and facility access.
- Managing project scope and conformance with System Quality Control, Statements of Work, Documentation, Implementation, and other Department requests
- Identifying project road blocks and working with management and team members for resolution
- Scheduling and facilitating all meetings concerning implementation and status checks

34. Proposer shall identify all contract staff positions by site location, position title, and job descriptions. (Section C.3.2.2.B)

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

As the current provider, CenturyLink has provided and will continue to provide dedicated staff that is qualified and fully trained in the performance of the contract. Since the implementation, acceptance and go-live of the contract, CenturyLink has met or exceeded TDCJ service level requirements. The table below details the positions and staffing levels that may change from time to time in order to continue to meet and exceed service level agreements.

Position Title	Location	Job Description
Account Manager	Huntsville, TX	<ul style="list-style-type: none"> ▪ Overall responsibility for performance of the OTS ▪ Customer advocate to CenturyLink Team management ▪ Commissioning and billing resolution ▪ Service and technical issue resolution ▪ Training, attendance at on-site meetings ▪ Promptly responding to Department and offender family requests, which shall include, but not be limited to e-mail, telephone and facsimile requests.
Alternate Account Manager	Dallas, TX	<p>Additionally, the CenturyLink Team already has assigned a full time Alternate Account Manager that will continue to be solely dedicated to TDCJ for the full term of the agreement. She works in coordination with the other Account Manager to fulfill all of the responsibilities listed above.</p>

Position Title	Location	Job Description
Service Representative and Data Administrator Manager	Dallas, TX	<ul style="list-style-type: none"> ▪ Responsible for installing, maintaining, and supporting the OTS system and additional products and service used by TDCJ ▪ Manage, hire and train all support personnel teams that provide customer service and technical support to TDCJ facility staff, as well as offenders and Friends and Family customers ▪ Promptly responding to Department when escalations occur ▪ Attendance at Department meetings when necessary ▪ Supports training initiatives for TDCJ personnel
Service Representative and Data Administrator Supervisor	Dallas, TX	<ul style="list-style-type: none"> ▪ Supports efforts to hire, train, and schedule all support personnel teams that provide customer service and technical support to TDCJ facility staff, as well as offenders and Friends and Family customers. ▪ Provides Level 3 escalation support.
Dispatcher	Dallas, TX	<ul style="list-style-type: none"> ▪ Manages all Field Technician dispatches for service issues and supervised PBI enrollments. ▪ Manages all TDCJ mailroom E-messaging/kite printing consumables ordering/deliver (paper, printer toner, drums, etc.)
Service Representatives	6 in the field at intake facilities Up to 12 (current staffing level) – Dallas, TX	<ul style="list-style-type: none"> ▪ General Customer Service to the Department ▪ Help Desk for Administrative support ▪ Data entry input - data integrity ▪ Intake Center enrollment/training of new offender's (field Service Reps) ▪ Updates to PIN, PAN, PBI enrollment (central Service Reps) ▪ Follow-up with the facility to insure all systems are operational and work is

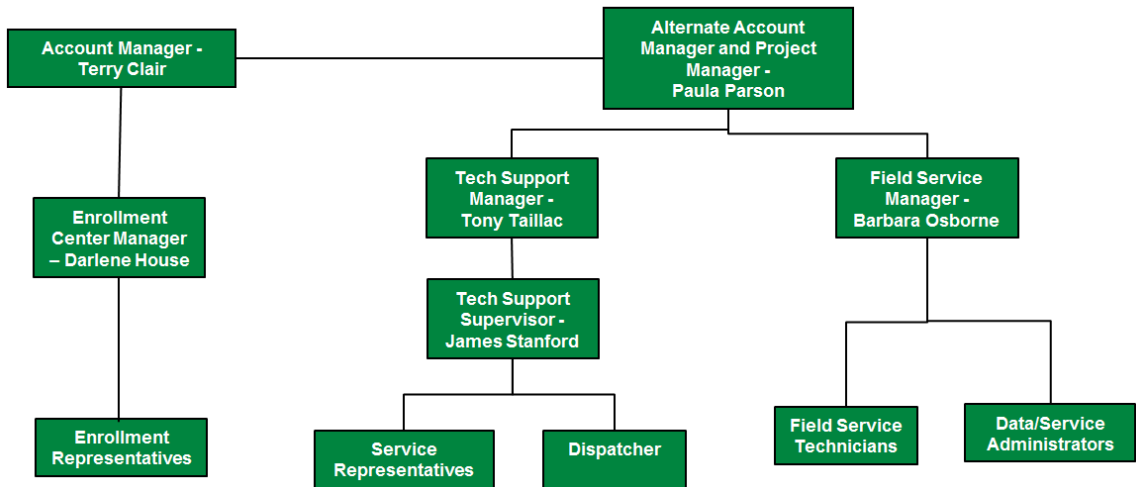
		<p>completed thoroughly and accurately</p> <ul style="list-style-type: none"> ▪ Administrative support of prepaid transactions ▪ Investigation of offender and staff complaints, processing of internal documents, and generating reports as requested ▪ Keeping accurate logs and documentation conveying messages and information in writing and/or via e-mail ▪ Advise management and open tracking tickets for all facility service affecting issues ▪ Help with effective operation of OTS components including hardware, software, and telephony equipment (when necessary).
<p>Data Administrators - 6</p>	<p>Dallas, TX</p>	<ul style="list-style-type: none"> ▪ Detailed troubleshooting/problem resolution as well as root cause analysis for all new and escalated tickets ▪ Responsible for accepting and/or assisting in problem analysis for Level 1 escalation ▪ Status customers on open issues and provide ETA of resolution ▪ Accurately document trouble tickets including root cause, problem analysis resolved and steps to final resolution ▪ Ensure resolution is verified with customer for all tickets before closure ▪ Work with Field Technicians to fully resolve problems ▪ Proactively maintain and scrub every system each time a troubleshooting event occurs ▪ Answer incoming customer and field technician calls • Ability to perform all functions of Level 1 Technician • Participation of on call rotation ▪ Provide mentoring to Level 1 technicians ▪

Position Title	Location	Job Description
Field Repair Site Technician Manager	Dallas	<ul style="list-style-type: none"> ▪ Supervision of fifteen Field Repair Technicians ▪ Oversee repair and maintenance ▪ Oversee initial PBI enrollment ▪ Customer advocate to CENTURYLINK Team management ▪ Attendance at Department meetings when necessary ▪ Promptly responding to Department when escalations occur
Field Repair Site Technicians – 15	In the field throughout TX	<ul style="list-style-type: none"> ▪ Maintain, repair and operate telecommunications hardware, LAN/WAN/Networking hardware/software, various electronic equipment and wiring per specifications and operational procedures at correctional facilities nationwide. ▪ Install, maintain, program and repair telecommunications hardware, associated LAN/WAN/Networking hardware/software, various electronic equipment and wiring per specifications and operational procedures. ▪ Work on a one-on-one basis with sworn facility staff, civilian facility staff, the offender population and the family members of offender's to resolve questions and concerns regarding billing, training, technical support and operational issues. ▪ Monitor and test equipment according to published equipment standards. ▪ Interface with all internal CenturyLink Team organizations, various vendors and contractors for problem solutions. ▪ respond to situations where standard procedures have failed in isolating or resolving problems. ▪ Required to complete TIA A+ Certification, as well as, a minimum of 2 years experience working with Cisco based routers, switches and PIX firewalls.

Position Title	Location	Job Description
Enrollment Center Manager	Tarboro, NC	<p>The CenturyLink Team has an Enrollment Center Manager already in place to continue service under this new contract. The Manager serves as an important point of contact for the Department for consumer service and security topics. The duties of the Manager include:</p> <ul style="list-style-type: none"> ▪ Overall responsibility for performance of the Enrollment Center ▪ Ensure all approved enrollments meet Department guidelines ▪ Manage Attorney Registration and Audit Process ▪ Manage Enrollment Center Representatives with progressive levels of responsibility to ensure all levels of support to the Department and offender Families are provided. ▪ Manage Offender Debit Refund Process. ▪ Promptly respond to escalations and requests from the Department, Attorneys, and offender families received by phone, email & facsimile. ▪ Interface with consumer billing service center management to coordinate approvals and consumer account management.
Enrollment Center Supervisors and representatives	Rocky Mount and Tarboro, NC	<p>The CenturyLink Team has existing full time Verification Representatives (currently 16) dedicated to the contract for the successful implementation of the friends and family enrollment project and ongoing support of the OTS. The Verification Representatives maintain a high level of ongoing customer service to all customers and ensure enrollments are processed in a timely manner. The primary duties of the Verification Representatives are:</p> <ul style="list-style-type: none"> ▪ Process each friend or family enrollment request received using the following methods: phone, fax, email or U.S. Mail. ▪ Troubleshoot and direct customers for quick and accurate resolution.

		<ul style="list-style-type: none"> ▪ Input customer account data and perform audits to ensure data integrity. ▪ Process Attorney registrations and conduct quarterly Attorney Audits Data to ensure data integrity. ▪ Process offender debit refund requests. ▪ Respond to email inquiries from offender families and the Department in a timely manner. ▪ Manually update the Department's daily block report
Digital Forensic Lab Staff	<p>2 Analysts – Austin, TX</p> <p>1 Liason – Austin, TX</p>	<p>The CenturyLink Team has a Cellular Forensics Laboratory; co-located with the Office of Inspector General (OIG) in Austin, TX, dedicate to TDCJ. The lab is currently staffed with 3 forensic examiners whose primary duties are:</p> <ul style="list-style-type: none"> ▪ Data extraction from recovered contraband cell phones ▪ Ad-hoc reporting of data extracted from contraband cell phones
Call Monitoring Staff (GEX) – TBD	Jefferson City, MO	<p>Guarded Exchange analysts are directly responsible for providing TDCJ investigative support by:</p> <ul style="list-style-type: none"> ▪ Call monitoring using investigative software with the purpose of identifying actionable leads ▪ Preparing reports based on their analysis
Trainers	Dallas, TX	<ul style="list-style-type: none"> ▪ Delivery of product training programs using a variety of training tools ▪ Conducting on-site customer training sessions ▪ Aligning product training to meet customer needs and expectations ▪ Defining content for training presentation materials ▪ Implementing standards and guidelines for customer product training ▪ Developing standardized customer training materials (instructors guides,

		training outlines and training syllabus) <ul style="list-style-type: none"> ▪ Delivery product Webinars ▪ Increase the Department's understanding and utilization of OTS ▪ Assess customer satisfaction with trainer and training
--	--	--



35. Proposer shall include, in detail, their Disaster Recovery Plan, which should also include a timeline. (Section C.3.3.B)

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The CenturyLink Team will continue to have complete end-to-end responsibility for all aspects of the service, including damaged or destroyed equipment due to natural disaster, lightning strikes, misuse of equipment, fire, or social insurrections.

As previously outlined, our OTS' centralized architecture is completely redundant and resilient. The most important advantages the CenturyLink Team can offer during a disaster or any other type of adverse condition are the safeguards inherent in the OTS itself. Redundancy is built in at the component level, the facility level, the network level, and system-wide. From automatic switching to a backup component, to dual VoIP providers, to customer data residing at multiple data centers in different parts of the country, each fail-safe is designed to ensure no loss of data.

Hundreds of hours of planning and a significant amount of capital have been invested in our disaster recovery approach to keep the OTS operational or able to recover as quickly as possible from disasters that may affect the Department. CenturyLink's Disaster Recovery and Continuity of Operations Plan is included on the following pages.

During recent hurricane events, we were at the ready to make emergency provisioning changes at TDCJ's request. Provisioning changes included extending calling hours 7am-10pm to 5am-12am daily and also adjusting Offender PIN restrictions to allow offenders to call from any facility to which they were evacuated.

Disaster Recovery & Continuity of Operations Plan

This CenturyLink Team has provided and will continue to provide the most advanced and dependable offender communications systems to Department facilities throughout Texas. This experience includes providing unmatched service and support to facilities through the worst of circumstances.

Our field team provides stability in these situations that cannot be matched or undervalued when the need arises. The CenturyLink Teams plans, as the Department does, to ensure proper operation in the face of adversity. Our disaster recovery plan is a valuable part of our solution when it is enacted.

If a catastrophic event, a natural disaster, or other system causes a loss of service to the Offender Telephone System (OTS), in order to provide consistent and high quality service to customers, the CenturyLink Team is prepared to carry out emergency response and recovery operations.

For TDCJ, the CenturyLink Team has a large dedicated account team dedicated to just the Department to assist whenever any problem occurs, including in times of disaster.

In the event of a disaster, the TDCJ team will also have the full support of our entire field service department, which includes 224 field service associates supported by a centralized field dispatch team. The Field Service Technicians (FST) are strategically positioned to support ongoing maintenance as well as any disaster recovery situations that our customers may encounter. The FSTs are trained and provided with disaster recovery processes, plans and checklists. The FSTs are supported by senior technical support resources and engineering in order to expedite repairs and minimize customer downtime.

Below is additional detail regarding processes that are in place to ensure effective responses for emergency and recovery operations. In addition, we are also including information on our preventative and security processes.

Securus System Control & Service Center

In order to provide protections that effectively lower the risk of loss of data, all data is stored in a centralized database and backed up offsite. Redundancy is a key component of the OTS. Our web-based system allows authorized users to access the data from any location with an Internet connection. The CenturyLink Team maintains the system at the highest level of operability.

The OTS provides a unique set of features that use advanced technology to store offender call recordings. Traditional premises-based calling platforms use local hard drives that may fail and are susceptible to local disasters, such as floods, tornadoes, hurricanes, and fires. The SCP uses 'SAN' (Storage Area Network) storage. SAN is a high-speed sub-network of shared storage devices. SAN's architecture avails all storage devices to all servers on LANs (Local Area Networks) or WANs (Wide Area Networks). Data on the SAN is stored in RAID (Redundant Arrays of Independent Disk) formats, spreading the data across multiple drives and providing additional protection. Data is no longer susceptible to loss due to an individual drive failure. Accordingly, SANs provide facilities with the ultimate protection against single drive or server failures, as well as increased security for each call recording.

The SCP is co-located in a Telx or AT&T Disaster Resistant Carrier Class Data Center that is managed under the direct supervision and immediate hands-on maintenance of data center personnel.

The call detail and call recordings are initially stored for on-line retrieval on multiple RAID's in two separate SANs. The system writes all recordings to each SAN, promoting disaster recovery in case of single disk or entire RAID failure.

Archiving to off-line is automated and managed by disc drives. A facility does not have to intervene or archive libraries. This automation removes the risk of human error.

Facility Emergency Response Checklists

The CenturyLink Team has developed procedures (checklists) to protect equipment and personnel in the event of an emergency situation. These procedures can be as simple as using sand bags to stabilize equipment and placing tape on windows that may be exposed to high winds. However, the effectiveness of these procedures can be affected by the lead time available to implement them. Earthquakes, flash floods, power outages etc., cannot be accurately forecasted. However, checklists will focus on mitigation and recovery. We will combine efforts between headquarters and field staff to expedite recovery wherever possible. Each checklist will be coordinated with the Department to ensure consistency with Department policy and procedures.

Spare Parts and Inventory Requirements

The CenturyLink Team requires that each field service site technician is equipped with a full inventory of spare parts kits for all equipment located at the customer premise. In addition, a backup inventory of spare parts is centrally located in Dallas, Texas, and at other strategically placed locations to ensure expedited response times. Finally, distribution agreements are in place with multiple vendors to provide expedited delivery service if necessary. The Securus corporate headquarters in Dallas, Texas, maintains a standardized emergency recovery package of frequently used spare parts and equipment that will be available for shipment to support failure backup efforts at our customer sites. Similar field spare parts kits are maintained by each of our technical field.

Response

Response operations will not begin until personnel safety can be assured. Emergency recovery operations are prioritized by critical facilities and equipment locations. The first priority is to recover maximum-security institutions and institutions with high offender phone usage. The preference of the customer is considered at all times. Field and headquarters management will ensure that responders are using all appropriate checklists and that the preparation for recovery operations is initiated within appropriate response guidelines.

Emergency Condition Declaration

The CenturyLink Team's Account Manager, Paula Parson, Technical Support Manager, Tony Taillac, and a predetermined designate from the Department will contact CenturyLink's General Manager to request a formal declaration of an emergency condition. Operations management will establish an immediate conference bridge with the appropriate participants to gather information substantiating that an emergency status is warranted and determining the level of response and actions.

The CenturyLink Team classifies disasters on a 1-3 level. Level 3 represents a moderate impact disaster and affects a small localized area. Level 2 represents a disaster that is high-impact and affects a more wide-spread area, which may include multiple facilities. A Level 1 disaster represents catastrophic events that are extremely wide-spread or affect a specific region with many facilities and customers.

If the information gathered from the call substantiates an emergency status, the emergency response level is determined. The following table defines the emergency condition levels:

Table: Emergency Response Condition Levels	
Condition Level	Response
Level 1	<p>Full headquarters response and possible deployment of a Headquarters Response Team to the region to coordinate and assist local recovery efforts.</p> <p>CenturyLink and Securus national field organizations are notified of the emergency situation. The Customer Service Manager and the Department initiate a Command Center, including CenturyLink and Securus Leadership. Necessary skill levels and geographic proximity are matched to the site's needs; additional personnel are dispatched as needed.</p>
Level 2	<p>Headquarters support will provide assistance to the local Recovery Team, as required to obtain internal Department support as necessary.</p> <p>On-site technician requirements assessed and additional personnel dispatched as necessary</p>
Level 3	<p>The local Recovery Team will coordinate all recovery operations. Headquarters assistance beyond normal technical assistance should not be required.</p>

Note: A Level 3 declaration notifies headquarters of the seriousness of an ongoing recovery effort, and provides the necessary background information if the local response team lead requests an upgrade to a higher condition level.

Our corporate headquarters will open a new trouble ticket in our ticket tracking system, indicating the declared condition level and the date and time of the declaration. All open tickets pertaining to the ongoing emergency recovery effort will be linked to the new trouble ticket and closed to ensure that all recovery efforts are recorded against a single ticket number.

Post-mortem reports are completed for all declared emergency condition levels. We analyze all post-mortem reports to advance our emergency recovery planning efforts.

Notification

Following the declaration of an emergency condition, the Securus National Service Center will continue to notify the Department using established notification and escalation procedures.

Offender Telephone System Failure Back-Up Escalation Plan

Emergency Contact Information

In addition to the dedicated TDCJ toll free support number that is already established and in use, the CenturyLink Team provides toll-free, 24-hour-a-day, 7-day-a-week emergency access phone number lists that will be readily available for use during an emergency situation. Additionally, conference bridges will be pre-established to facilitate group communications. Contact information will be updated at regular intervals to ensure accuracy. The Securus National Service Center will also maintain these emergency contact phone number lists and

coordinate on a regular basis with field staff to ensure that all lists are accurate. Notification based on pre-established timelines and contact lists will occur via email notification and/or an outbound auto dialer.

The CenturyLink Team understands that emergencies don't just occur outside the perimeter, often times the emergency takes place within a facility. As a result we offer to engage the Department in a program for an Emergency Notification Service. The Service would utilize CenturyLink's enterprise auto-dialing system to perform mass notifications in case of an emergency. One example of an application is a mass callout to staff during a security emergency. Using a pre-populated list by Unit, authorized Department personnel would have access to 24/7 on-call personnel to initiate a callout. A key feature of the auto-dialer is its ability to repeatedly attempt callouts until the call is received by a live person; i.e. if a call goes to voicemail, the system will continue to attempt that number until answered.

Technical Support

The CenturyLink Team understands that throughout the duration of a critical event, our customers rely on our support to guide them with minimal loss of equipment and data. Qualified resources will be available to assist the Department. These resources include the TDCJ account team in add to the more than 224 full-time field technicians who can deploy nationwide, and a full list of contacts.

We also realize that during a disaster, it may be even more important that offenders and detainees can stay in contact with their friends and family. To support these end users, Securus maintains two fully staffed Technical Support Centers in Dallas, TX and Atlanta, GA that can continue call processing, even if there is a failure at one location.

Coordination

Coordination of all declared emergencies will depend on the emergency level. Field staff will coordinate the emergency response to all level 3 conditions. Headquarters will provide assistance at the request of field management for Level 2 emergency conditions, and will coordinate all Level 1 emergency efforts.

The field management team will develop mutual agreements with other Securus regions in the country or with vendors to supply resources, equipment, or manpower. Additional equipment and personnel may not arrive for several days, depending on available transportation, condition of the roadways and airports, and other factors, therefore, field management will not delay the decision to ask for assistance from other sources.

Mobilization

Mobilization of a Headquarters Response Team, if necessary, will depend on need, as determined by the headquarters and field management.

The Headquarters Response Team will be dispatched from Dallas as soon as possible to assist field recovery efforts. However, field staff will begin recovery operations without delay

Emergency Response Teams

The following teams will be formed to respond to declared emergency conditions. These teams will include subject matter experts and necessary support staff.

Table: Emergency Response Teams	
Team	Manning and Responsibility
Field Local Recovery Team	Plans and directs local recovery operations. Staffed by field staff personnel only.
Headquarters Support Team	Provides technical support and assistance to local recovery teams. Staffed cross-functionally, as required.
Headquarters Response Team	Deployed to Securus local markets to assist local recovery operations. The Headquarters Response Team is staffed by subject-matter experts and led by headquarters operations management.

Recovery

Recovery operations may last several hours, several days, several weeks, or longer. Field staff will continue recovery operations until critical offender calling functions have been recovered and restored to normal call and data transmission capability. When emergency operations are no longer necessary, the Headquarters Response Team will be recalled, but minor recovery operations may still continue.

Throughout emergency recovery operations, the headquarters and field staff record all recovery actions and results. Following the resolution of emergency response operations, all recovery teams and appropriate management submit pertinent information and comments to be included in the Post Mortem report.

With virtually all of the data, such as call records, recordings and system settings residing in redundant databases at the centralized sites, the CenturyLink Team is confident that the Department will not lose data following restoration of the OTS. Additionally, our OTS is one the most stable calling platforms in the industry with nearly perfect, 100% availability. Through design, proactive monitoring, and rapid-response procedures, Securus minimizes customer-impacting outages.

Risk Mitigation and Proactive Monitoring

The SCP platform and infrastructure was 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 and Network

Securus continuously monitors all data centers, infrastructure components, platform systems and Offender Telephone Systems (OTS) 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.

- 36. Proposer shall describe, in detail, the method that will be used to transfer data and associated files and records to the Department. (Section C.3.3.C)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

TDCJ and CenturyLink have worked closely together to establish the methods that are being used to successfully transfer data and associated files and records. This already established method of data transfer will be retained under any new contract. CenturyLink looks forward to working with the Department to enhance or change any data exchange method in the future. As an example, enhanced methods may include new files and records that may be required for the new video visitation solution requested by the Department. CenturyLink is prepared to develop any new methods, protocols, process and procedures resulting from this new contract.

Integration Process

The dedicated Securus Integration team has designed, developed, tested and implemented all custom integrations for the Department to deliver a fast and flexible solution.

We have an established interface with the State that provides a current roster on a daily basis. This occurs through database extract in CSV format via SFTP. The e-imports function within SCP takes transmitted information and populates the appropriate fields within the SCP system without further intervention from TDCJ staff.

The files that we currently receive from TDCJ through this integration include:

- Booked Files - Received Daily in order to create/reactivate offender accounts, update facility/PIN and manage activation/deactivation of suspensions.
- Complete File of All Offenders and their Current Status – Performed Monthly to ensure all offender files are the most up to date.
- Release Files: Received daily and automatically deactivates offender accounts as offenders are released from TDCJ.
- Change Account – Received weekly, providing information for changed offender account numbers and updating the system automatically.
- Debit File – Received daily providing commissary purchase information in order to update the debit account.

The Booked, Complete and Release files transmit the information to include the following fields.

- SiteID
- Account Number
- Last Name, First Name
- Middle Name
- PIN
- Suspension status

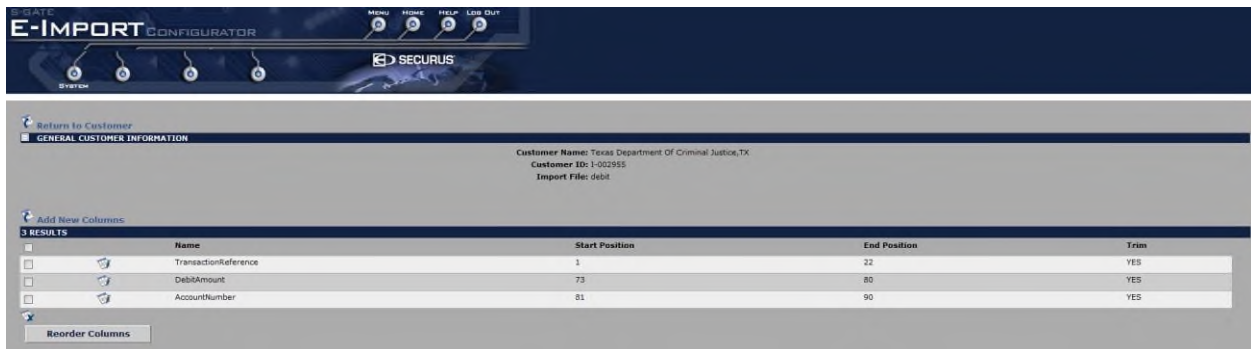


Customer Name: Texas Department Of Criminal Justice, TX
 Customer ID: 1-002955
 Import File: booked

Name	Start Position	End Position	Trim
SiteID	1	6	YES
AccountNumber	7	15	YES
LastName	16	41	YES
FirstName	42	67	YES
MiddleName	68	88	YES
PIN	89	97	YES
Suspend	98	99	YES

The debit file transmits the information to include the following fields.

- Transaction Reference Number
- Debit Amount
- Offender's Account Number



Customer Name: Texas Department Of Criminal Justice, TX
 Customer ID: 1-002955
 Import File: debit

Name	Start Position	End Position	Trim
TransactionReference	1	22	YES
DebitAmount	73	80	YES
AccountNumber	81	90	YES

The Change Account transmits the information to include the following fields.

- Old Account Number
- New Account Number



37. Proposer shall describe, in detail, how the Offender account requirements will be accomplished. (Section C.3.3.E.1)

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The CenturyLink Team will continue with the current process of funding offender telephone accounts. There are two main methods of doing so; 1) by the offender purchasing “debit” time through their commissary account, or 2) Friends and Family directly funding the account just like they do for their prepaid Collect accounts through one of the following outlets:

- Call our Customer Service center and speak with a live operator
- Use our automated interactive voice response system
- Use our mobile-friendly website
- Fund accounts by mail
- Visit one of more than 35,000 MoneyGram locations such as Walmart and CVS Pharmacy
- Visit one of more than 58,000 Western Union locations.

Today we complete approximately 20,000 debit funding transfers per month for TDCJ offenders

- Charges appear on a bill generated by Securus Correctional Billing Services (Securus customer service and billing division). Called parties are subject to credit checks (as allowed by state regulations) to set up a direct billed account.

Prepaid Accounts

We offer friends and family members of offenders a wide variety of options to set up and fund prepaid accounts. Called parties fund these accounts in advance and charges are deducted from an account as calls are made.

To create and fund a pre-paid calling account, friends and family members can:

- Call our Customer Service center and speak with a live operator
- Use our automated interactive voice response system
- Use our mobile-friendly website
- Fund accounts by mail
- Visit one of more than 35,000 MoneyGram locations such as Walmart and CVS Pharmacy
- Visit one of more than 58,000 Western Union locations.

In addition, prepaid accounts can be funded through JPay, just as friends and family fund trust deposits for TDCJ offenders today.

Billing and Account Management

Customers can use our toll-free number to either speak to a live agent or use an intuitive, automated interactive voice response system to help them with their billing needs. Live agent support is available to friends and family members seven days a week, 24 hours a day, and 365 days a year. For added convenience, we also offer personal account access via our website (www.securustechnologies.com). End-users can also access customer service via online “chat” 24 hours a day, seven days a week.

Our friendly and knowledgeable agents can help customers with:

- Setting up and funding accounts
- Making payment arrangements
- Obtaining information on credit limits
- Resolving complaints
- Blocking and unblocking numbers
- Reviewing call durations and history
- Learning about MoneyGram® options
- Learning about Western Union® options
- Receiving information on new services
- Confirming originating facility
- Reviewing account balances
- Answering questions and helping customers with refund requests
- Managing account notifications

Our customer service agents are highly trained on OTS issues and in satisfying the specific needs of called parties. We offer both English speaking and Spanish speaking agents.

Fees

We will not charge set-up fees for called parties who create pre-paid accounts. Friends and family members also have the option to fund accounts with no fees and to avoid minimum funding requirements. The current low fee structure in place at TDCJ today will continue.

Ancillary Service Charges and Other Fees

Securus' Ancillary Service Charges (see 47 C.F.R. § 64.6020) and other fees to Consumers relating to the use of its offender calling services are as follows:

Fees Vary by Account Types*	How Applied	Amount	Account Type
Account Set Up	At account initiation	\$0.00 Always Free	Any Account
Payments via mail or online banking	Each payment	\$0.00 Always Free	Any payment to any Securus account
Paper Bill/Statement Fees	When choosing local carriers to bill, applied once/month when used for a paper bill or statement. Does not apply to electronic bills/statements.	\$2.00	Direct Bill only. Prepaid Statements are available at no charge.
Automated Payment Fees	For automated payment by phone or website	\$3.00	For payments to prepaid (AdvanceConnect and Inmate Debit) and Direct Bill accounts
Live Agent Fee	For payment through a live agent	\$5.95	For payments to prepaid (AdvanceConnect and Offender Debit) and Direct Bill accounts
Return Check Charge	Applies to any checks returned for insufficient funds.	Up to \$25.00, depending on state regulatory rules	For payments to prepaid (AdvanceConnect and Offender Debit) and Direct Bill accounts

* Sales taxes, Universal Service fund fees, Telecommunications Relay Service (TRS) fees may also apply, based on local, state, and federal taxing authorities.

Certain third-parties may charge the following fees:

- MoneyGram: \$10.99
- Western Union: \$11.95

Friends and Family Obtaining a Refund

To obtain an account refund, end users may contact Customer Service by phone, or by chat at www.securustech.net. For all credit card transactions made by phone or website, full and partial refunds will be applied to the payment source last used. For full refunds on accounts last funded via Western Union, funds will be refunded to the customer through Western Union. For partial refunds on accounts funded via Western Union and for both full and partial refunds on payments mailed to Securus, a check will be mailed via the U.S. Postal Service. Full refund amounts are available at no charge up to one year of date of last use. Unclaimed funds, including pre-paid funds, will be remitted to the State through an established escheatment process.

39. Proposer shall describe, in detail, how they called party registration requirements will be accomplished. (Section C.3.3.F.1)

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The Called Party registration process has been custom-developed by CenturyLink in consultation with TDCJ staff over the past 9 years, exceeding the requirements contained in C.3.3.F.1. For this process, CenturyLink staffs a TDCJ-dedicated center staffed primarily out of Rocky Mount and Tarboro, NC.

Highlights of the registration process:

- Custom web page at texasprisonphone.com
- Enrollment options online, toll-free automated phone or live representative, and by mail
- Confirmation of eligibility and acknowledgement of rules (including all those contained in C.3.3.F.1)
- Custom development of service representative UI and database for consumer management and data gathering
- Custom development of Interactive Voice Response system and prompts
- Strict adherence to TDCJ security guidelines
- Coordination with TDCJ staff for members of the State's Victims List
- Strict management of customer eligibility, including prohibition of registering another number of blocked by authorized TDCJ staff
- Ongoing audits of eligible numbers due to number portability
- Data held for TDCJ investigative purposes

The enrollment process has evolved over 9 years and is 100% custom to TDCJ. During this time, we believe the State would agree CenturyLink has delivered outstanding service to family members in addition to TDCJ. Continuing with CenturyLink would preserve all historical data in their native format and, most important, the processes and service relationships that TDCJ has counted on during the prior contract.

We highlight the management of eligibility requirements, which have evolved over time through discussions with TDCJ OTS management staff and CenturyLink management. Management of these requirements involves loading the database with prohibited "Operator Carrier Numbers" (OCNs) within the Line Information Database (LIDB) to disallow nomadic VoIP services like Magic Jack. It also involves 3-way calls with cell phone carriers for ALL cell phone enrollments – this is necessary because LIDB and other carrier databases do not distinguish between prepaid and postpaid cell phone services.

General Description: Enrollment Center and Back Office Processes

Customers are required to accept five terms before their enrollment can be approved. CenturyLink maintains documentation of the terms accepted for TDCJ review at any time.

As part of our enrollment process, center representatives verify the name against the Texas Driver's License Bureau. This requires maintenance of Texas DL data and purchase of data updates from the State of Texas.

The process then verifies the offender against TDCJ active offenders list, in addition to verifying the applicant's name and type of service with their carrier before approval. This requires a LIDB and Calling Name (CNAM) dip for each customer. For applicants attempting to enroll a post-paid cell phone, enrollment requires a copy of their phone bill or a third-party call to their carrier to verify account name and pre-paid/post-paid status. These three way calls can be lengthy depending on the cell phone provider, and our representatives maintain live contact throughout the process. As stated previously, the name on the customer's driver's license is verified against the phone bill owner.

CenturyLink carefully manages fraudulent attempts to enroll, which are significant in number. Suspicious/fraudulent attempts are flagged within our system, and follow-up attempts require manual intervention, including review of signatures among different forms, and other checks.

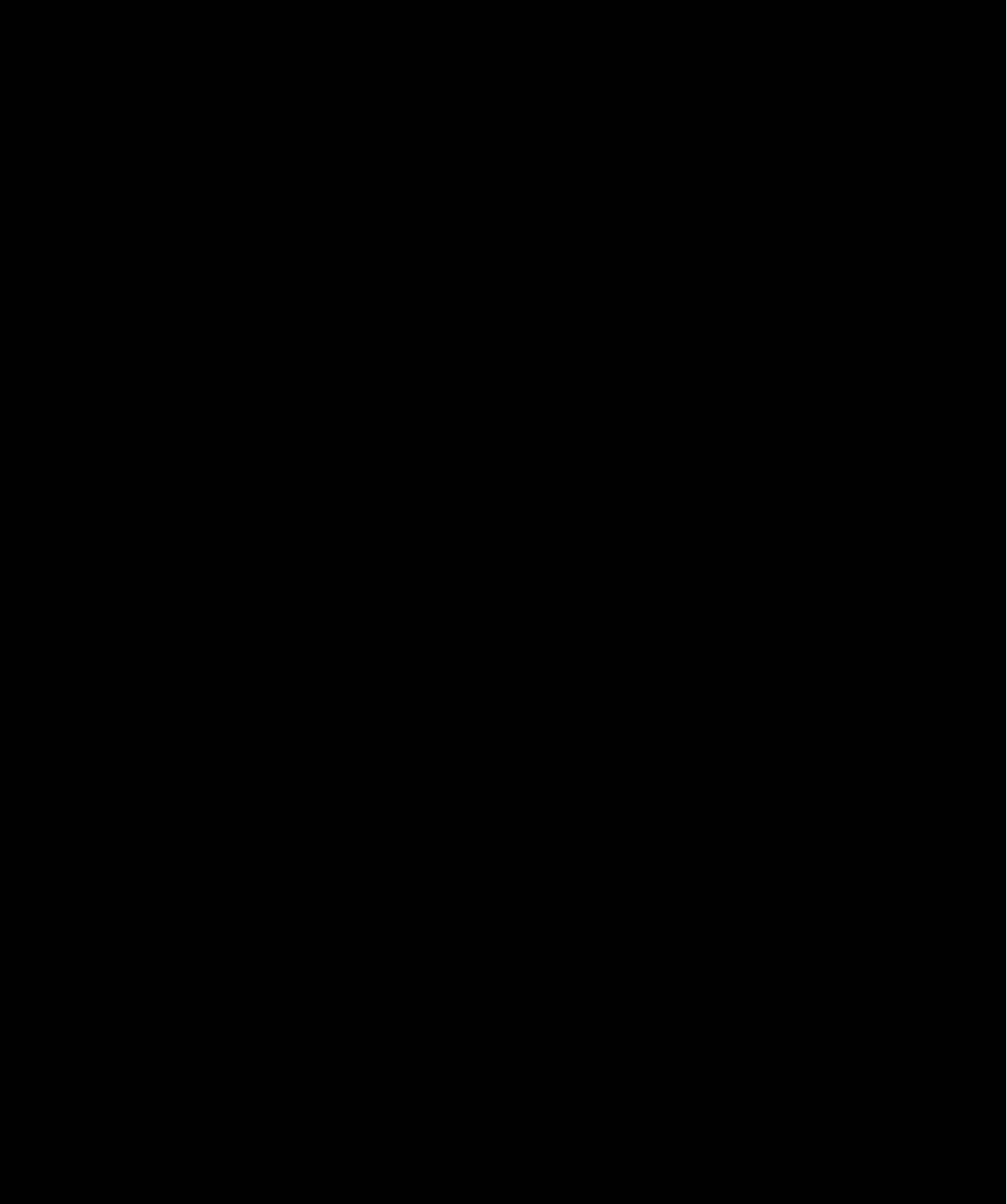
Business owners are not allowed to register their phone numbers if they are listed as corporations or LLC. Small business owners can register their phone number but their name has to be on the phone bill with a DBA or without the word "attention" or "care of". The only method a small business owner can register their phone number is via phone enrollment.

Once we have confirmed that the customer meets TDCJ requirements, we send a nightly list of those customers to TDCJ to verify against the victims list before final approval. Once we receive final approval, we update accounts to make them eligible to receive calls, and send an email to consumers regarding their application status.

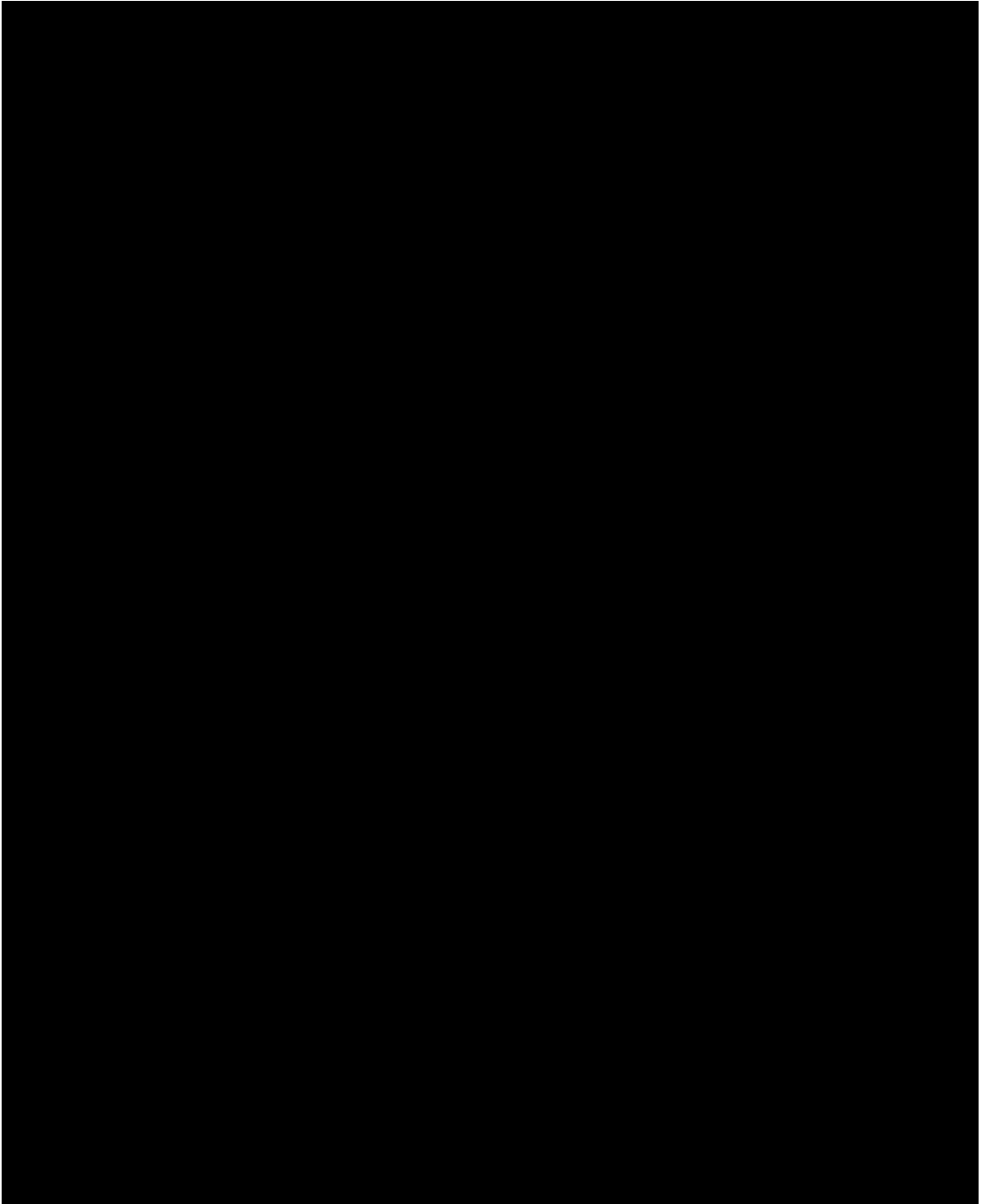
This process occurs for each individual number attempting to register for each eligible offender.

As TDCJ is aware there are multiple processes for different service types – for the convenience of the Department, the proprietary/confidential Live Rep and Offline processes are provided below.

Cell Phone Enrollment – Live Rep



Cell Phone Enrollment – Offline



The Enrollment Center also manages several important post-enrollment processes to maintain security on an ongoing basis. The two most important of these are TDCJ blocking management and number audits.

TDCJ block management

When TDCJ blocks a customer from receiving calls from an offender, CenturyLink further ensures the customer is not allowed to register any other numbers for that offender, as well as ensuring no other customers are allowed to enroll numbers using the same address that the blocked customer used on the initial enrollment. This takes additional special programming and some manual intervention to ensure the blocked customer does not gain access to the offender via the OTS.

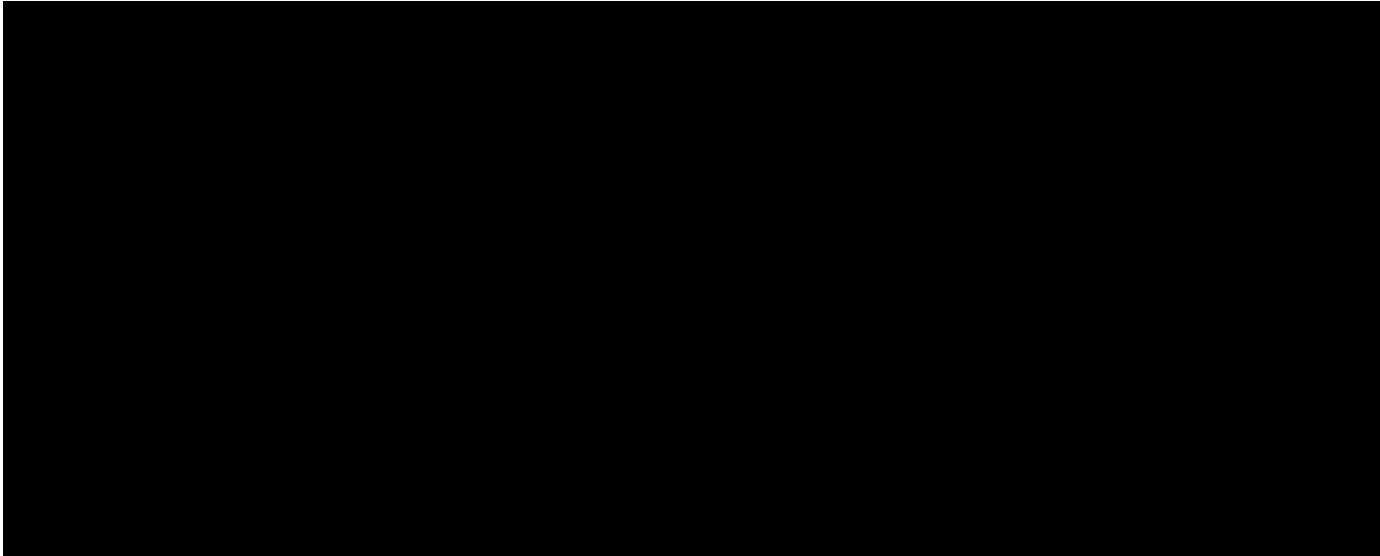
Ongoing audits

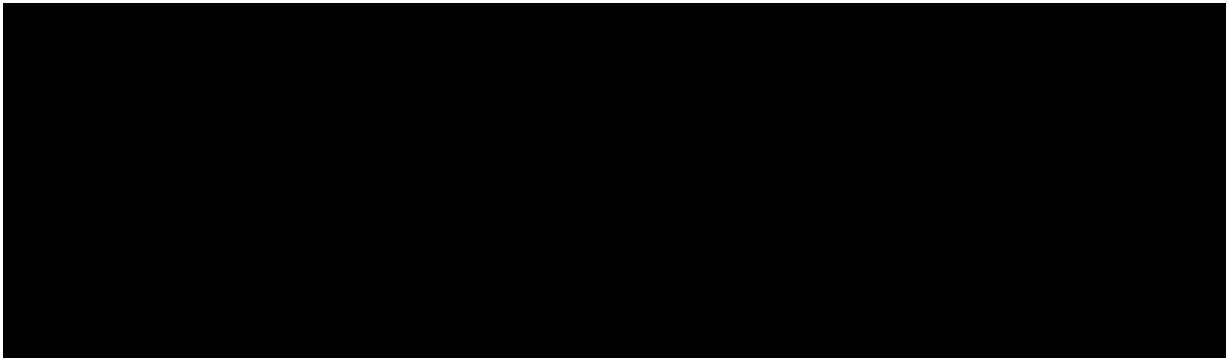
CenturyLink receives daily booked, release, and update files from TDCJ to maintain an active offenders list and to update customer account status. We also receive a monthly active offenders list as a method to audit these daily updates, and perform other periodic audits for TDCJ. These include monthly audits of 10% of F&F accounts (all eligible PANs audited at least once annually). Cell phone customers who have changed carriers are automatically deactivated and required to re-enroll. Finally, we perform quarterly attorney audits where we verify “Do No Record” of attorney numbers and also verify attorney standing with the Texas Bar.

- 40. Proposer shall describe, in detail, how the attorney registration requirements will be accomplished. (Section C.3.3.F.2)**

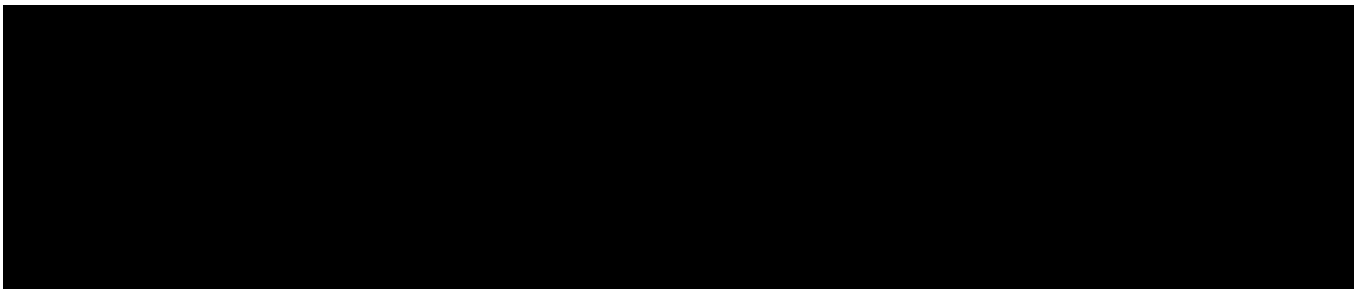
CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

Similar to Called Party registrations, attorney numbers are subjected to rigorous verification. The importance of this process is obvious, since it is used to maintain attorney-client privilege.





Attorney Audit Process



41. Proposer shall describe, in detail, the plan for problem resolution forms. (Section C.3.3.G)

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The CenturyLink Team has worked extensively with the Department to establish and refine the problem resolution process for instances when issues arise or when offenders have questions about the system, which includes:

- Establishing a Technical Support Department dedicated solely to problem resolution for TDCJ,
- Creating and polishing the Assistance Request Form into its current format, and
- Establishing and refining Assistant Request processes and procedures (Kites).

The CenturyLink Team will continue to provide and maintain the necessary work stations and equipment necessary for scanning and transmitting the resolution forms. We currently print the Assistance Request Form on the agreed upon pink paper and provide them in bulk to the Department, along with other consumable supplies, like toner. Our technical support team will make sure the Department is always properly stocked of these supplies.

The CenturyLink Team will provide an initial response confirming receipt of the problem resolution form, if not the problem resolution itself, within one (1) business day submission. The CenturyLink Team does not charge for the transmission or response to a request for assistance.

Kites

Assistance Request forms (aka - kites) are available at all TDCJ facilities for offenders to use when they have questions on how to use the OTS or have any OTS issue that needs to be addressed.

- Step 1: An offender fills out and submits a kite at their facility's mailroom.
- Step 2: Mailroom personnel scan the offender kites using a workstation and scanner that have been provided by JPay. Each time a kite is scanned using the supplied Jpay eMessaging system, it is delivered to a dedicated TDCJ support Service Representative.
- Step 3: The Service Representative reviews the scanned kite and begins researching the issue. They will craft a response for the offender and submit it back to the offender using the Jpay eMessaging system.
- Step 4: The facility mailroom personnel receives the offender kite with the Service Representative's response and prints it out to deliver to the offender.

TDCJ Offender Telephone System (OTS) - Assistance Request Form

INSTRUCTIONS	COMMON PROBLEMS	RECOMMENDED RESPONSE	
<ul style="list-style-type: none"> ◆ Review list of common problems before submitting a complaint form. ◆ This form is to be completed and placed in a unit mailbox to be picked up by the mail room. ◆ You must print legibly. ◆ Expected response should be 7-9 business days after the form has been placed in the mailbox. ◆ List only one issue per form. ◆ Incomplete or unreadable forms will be returned unresolved. ◆ Please do not submit multiple forms on the same issue. Forms will be addressed and responses will be sent out in the order in which they are received. 	My TDCJ # does not work.	Please make sure you are entering your full 8 digit TDCJ ID # including leading zero(s) if needed.	<div style="border: 1px solid black; width: 100%; height: 100%; background-color: black;"></div> <p style="font-size: small; text-align: center;">Please write your TDCJ-ID# in the squares and then completely fill in the corresponding number boxes above, including leading zero(s) if needed.</p>
	Message says "...this number is not authorized..."	The owner of the phone number you are attempting to call must register their number by calling 866-806-7804 or by going to www.texasprisonphone.com .	
	Message says "...could not verify your name..."	If you routinely receive these messages, you may need to be re-enrolled into the Voice Biometric System. Please submit this form with a description of your problem.	
	Message says "...your enrollment does not exist..."	You are not enrolled in the OTS Voice Biometric System. You do not need to submit this form. We will identify all eligible offenders that are not-enrolled and will schedule enrollment periods at least every two weeks.	
	Message says "...your account has been suspended..."	Phone accounts will automatically be suspended for 90 days on conviction of a major disciplinary. Offenders in transient status will also be suspended. No calls can be made until your status has been cleared. OTS representatives are not able to answer questions about offender suspensions.	

Offender Name (Last, First, MI)	Today's Date	TDCJ Unit Name	Telephone Number Called
Explanation of Issue (Be specific, include details)			
**** TO BE COMPLETED BY TECHNICAL SUPPORT ****			

Stock # 706-01-19251-0 TX 005 July 2011

The Assistance Request Form includes a list of frequently asked questions and answer for the offender.

When the CenturyLink Team began its relationship with the Department, kites had to be physically mailed to our service technicians. This method was inefficient and dangerous for mail room personnel. Seeing an opportunity for improvement, we digitized the kite process by providing workstations in the TDCJ mailrooms and training for staff on how to electronically send kites to the dedicated TDCJ service center. This enhanced method will continue under any new contract.

**42. Proposer shall describe, in detail, the plan for a digital forensics service.
(Section C.1.1.X)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The CenturyLink Team is proud to propose the continued use of your fully functioning Cellular Forensics Laboratory; co-located with the Office of Inspector General (OIG) in Austin, TX. This state-of-the-art Cellular Forensics Lab is part of a comprehensive suite of investigative solutions. The Cellular Forensics service allows TDCJ to maintain and improve upon your ability to retrieve saved and deleted information such as call logs, messages, contact information, photos, videos, browser history and SIM/SD card analysis from recovered contraband cell phones.

Cellular Forensics brings a unique examination capability to the Department for recovered contraband cell phones. Examiners provide a comprehensive and analytical breakdown of the cellular data using Cellebrite and several other computer forensic programs—such as Encase, Internet Evidence Finder, Passware, Oxygen Phone Forensic Suite, Forensic Explorer—that can also perform in-depth forensic analysis on acquired devices and any form of digital media.

Our solution uses the most advanced technology available to integrate all recovered information into a single, cohesive source with the sole purpose of helping the Department generate Actionable Intelligence™. The Cellular Forensics Lab is powered by forensics grade computers and it maintains all commercial software licensing in accordance with the Department's 1 for 1 license to staff member ratio. The Lab has been a great success at TDCJ and will continue to be offered under any new contract with staffing and systems deployed to process 150 to 200 phones per month. The Lab will continue to be staffed with three certified forensic examiners who have already obtained the necessary employment clearances from the OIG. If the volume changes over time, we will work with the Department to ensure appropriate staffing levels.

Our Forensic Examiners are also certified to perform data extraction of devices that are damaged, locked, or unsupported by other forensic tools using the latest Chip-Off Forensics technique. Chip-Off Forensics is the process of removing the flash memory from the printed circuit board of a device using either a heat or no-heat method, depending on the purpose of the extraction, and reading and analyzing the raw data stored on the chip. This process allows the Department to access more locked and damaged devices, increasing the potential intelligence and data gathered from devices.

The combined experience of our Forensic Staff, along with industry-leading hardware and software, provides the highest quality of digital forensic services on mobile devices, and any digital media.

Finally, forensic lab personnel will continue to employ strict Chain of Custody and evidence security procedures to safeguard all evidence within its possession. These policies and procedures are designed and maintained throughout the process from receiving of the evidence, data extraction and return of the evidence. These Mobile Device policies and procedures are based upon the best practices recommended by Cellebrite, an industry recognized leader in the field, with input and approval from the Department.

Every item received by Guarded Exchange Forensic services is entered into an electronic spreadsheet as well as individually labeled and attached to a Acquired Property form, where custody within the Guarded Exchange offices is maintained and documented. The Guarded Exchange forensic lab and evidence room is a locked, secure room with access limited to staff approved. A copy of the Guarded Exchange Forensic Services Policies and Procedures guide is available upon request.

- 43. Proposer shall include, in detail, their comprehensive time schedule that outlines the entire project from award of Contract to full operational status in the comprehensive Implementation Plan.(Section C.3.4.1)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

Building upon the success of the original OTS installation, the CenturyLink Team is providing our Implementation Plan to update the Departments OTS workstations, offender phones and network infrastructure in addition to 120 video visitation units. This technology refresh effort will provide the TDCJ with the technology and tools to support the Department's OTS mission today and throughout the life of the contract. It will provide the technology infrastructure necessary to implement the additional products and services outlined in this proposal and will allow the CenturyLink Team to enhance the quality of products and services to the Department.

The CenturyLink Team, as the first ever OTS provider, is the most qualified to support the implementation requirements of this proposal and benefits from a unique understanding of the complexities associated with managing the OTS at the Department's 114 facilities statewide. We understand the herculean effort that was required to install the Departments first OTS, from its inception through final acceptance, while working diligently to meet the operational expectations of the Department and the associated service level agreements (SLAs) required by the initial contract.

We will build upon the initial installation success that saw 5,439 OTS phones installed at 114 TDCJ facilities in approximately nine (9) months. An effort that consumed almost 922,000 hours from more than 100 associates to install the technology infrastructure required to offer the OTS to TDCJ offenders. In addition, we enrolled over 122,000 offenders to the OTS using a voice biometric technology and implemented investigative capabilities that were never been available to the Department.

That is the shared legacy of the TDCJ and CenturyLink Team partnership. We offer the following implementation Plan as a means of continuing this relationship for the next decade and beyond.

The CenturyLink Team Legacy:

- 5,439 OTS Phones
- 114 Facilities
- 100+ Associates
- 921,866 Hours
- 9 Month Installation
- 122,155 Offenders Served
- 299,817 Offenders Enrolled

ID	Task Name	Duration	Start	Finish
1	CenturyLink Offender Calling System Installation Project Plan for Texas Department of Criminal Justice	191 days	Tue 9/4/18	Tue 5/28/19
2	Offender Calling System Installation & Cut-Over	191 days	Tue 9/4/18	Tue 5/28/19
3	Project Initiation Phase	6 days	Tue 9/4/18	Tue 9/11/18
4	On Site Kick-Off meeting with TDCJ & CenturyLink Account Team	3 days	Tue 9/4/18	Thu 9/6/18
5	Site Surveys conducted by CenturyLink Field Services Team (Mandatory)	3 days	Fri 9/7/18	Tue 9/11/18
6	Project Planning Phase	71 days	Thu 9/13/18	Thu 12/20/18
7	Engineering Schematics, Bill of Materials, and Manual of Procedure (MOP) Updates	7 days	Thu 9/13/18	Fri 9/21/18
8	Agency Provisioning and Data Management	55 days	Mon 9/24/18	Fri 12/7/18
9	Product and feature provisioning within the operational platforms	70 days	Fri 9/14/18	Thu 12/20/18
10	Hardware and LEC transport orders	14 days	Fri 9/14/18	Wed 10/3/18
11	Project Execution Phase	137 days	Fri 10/5/18	Mon 4/15/19
12	Delivery confirmations	82 days	Fri 10/5/18	Mon 1/28/19
13	LEC Circuit deliveries (As Necessary)	70 days	Fri 10/5/18	Thu 1/10/19
14	Hardware deliveries throughout DOC	68 days	Thu 10/25/18	Mon 1/28/19
15	Pre-Installation activities per facility	67 days	Mon 11/19/18	Tue 2/19/19
16	Verification of shipment content to pick list	66 days	Mon 11/19/18	Mon 2/18/19
17	Process received hardware paperwork	66 days	Tue 11/20/18	Tue 2/19/19
18	Installation activities per facility	99 days	Wed 11/21/18	Mon 4/8/19
19	Installation of all required hardware in phone room and through the facility	96 days	Wed 11/21/18	Wed 4/3/19
20	Installation of all phones by pod or dorm	98 days	Thu 11/22/18	Mon 4/8/19
21	Installation of additional workstations	96 days	Fri 11/23/18	Fri 4/5/19
22	Installation of Video Visitation at designated 12 locations	96 days	Fri 11/23/18	Fri 4/5/19
23	Training of product and feature utilities	15 days	Tue 3/26/19	Mon 4/15/19
24	Walkthrough of product details by user group access	15 days	Tue 3/26/19	Mon 4/15/19
25	Agency training certifications by user group	15 days	Tue 3/26/19	Mon 4/15/19
26	Controlling and Monitoring Phase	104 days	Wed 12/5/18	Mon 4/29/19
27	Perform Change checkpoints	90 days	Wed 12/19/18	Tue 4/23/19
28	Identify change orders for specific facility requirements not identified at Site Survey	90 days	Wed 12/19/18	Tue 4/23/19
29	Quality evaluation checkpoints	104 days	Wed 12/5/18	Mon 4/29/19
30	Verification of project installation activity by facility	104 days	Wed 12/5/18	Mon 4/29/19
31	Complete checklists and document connectivity and utilization per facility	104 days	Wed 12/5/18	Mon 4/29/19
32	Closing Phase	34 days	Thu 4/11/19	Tue 5/28/19
33	Cutover of product and features to calling platform	19 days	Thu 4/11/19	Tue 5/7/19
34	Reverification of services are functional	15 days	Thu 4/11/19	Wed 5/1/19

ID	Task Name	Duration	Start	Finish
35	Cut sheet distribution	4 days	Thu 5/2/19	Tue 5/7/19
36	Post cutover activities	15 days	Wed 5/8/19	Tue 5/28/19
37	Open project tickets for post cutover monitoring	15 days	Wed 5/8/19	Tue 5/28/19
38	Monitor site activities of product functionality	15 days	Wed 5/8/19	Tue 5/28/19
39	Agency acceptance and project closure	15 days	Wed 5/8/19	Tue 5/28/19

44. Proposer shall include, in detail, their comprehensive plan that outlines the installation. (Section C.3.4.2)

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

As the incumbent provider, many of the installation activities associated with a non-incumbent provider, such as hiring and training of new staff, transfer of call records and recordings, setting up new data transfers, new telephone lines and additional time of Department staff, **will be minimized** if the CenturyLink Team remains your OTS provider.

Our offer includes the installation of all new telephone units. The CenturyLink Team will evaluate the condition of all other hardware and provide all additional wiring, cabling, conduit, cross-connects, jacks, plates, and related hardware, necessary for the system to operate to the latest generation at no cost to the Department. We assign fully qualified, factory-trained field technicians to inspect shipped equipment, and install and maintain SCP for the duration of the contract period.

We have a proven track record of providing successful turnkey installations for large State Department of Corrections agencies, including new services being installed at TDCJ. This success stems from utilizing generally accepted telephone industry installation practices. Our extensive experience installing and maintaining inmate communication systems has helped us develop installation and cut-over procedures that will minimize disruptions and errors, and allow your system to come online with little or no staff involvement.

Process

At the beginning of the new contract term the CenturyLink Team will meet with the Department to discuss implementation and installation. We are expecting the Department to select a number of Added Value products and services that we have offered. Depending on the Added Value services selected and quantities, the CenturyLink Team will work closely with the Department to finalize and schedule the Implementation Plan. We have provided a preliminary Implementation Plan and Transition Schedule in response to Question 43 that provides a schedule of implementation, illustrating the date and time for start of installation and a date certain for the system and equipment to be fully operational and providing services.

The CenturyLink Team understands the installation requirements enumerated in Section C.3.4.2 and will comply. As the incumbent provider, the CenturyLink Team has good understanding and knowledge of the Department's infrastructure, applicable electrical codes, Department policies, security guidelines and rules. Wherever possible, Securus will avoid work that requires cutting into or through girders, beam, etc. Wherever possible, we will re-use existing station cabling and where existing station cabling cannot be used, we will install new station cabling at no cost to the Department.

Throughout the duration of the project, our Project Management Team will provide weekly installation progress reports. The reports will include updates on all active, completed, and pending installation activities.

During the cut-over, the CenturyLink Team will perform a thorough inspection of the installation and will resolve any potential issues prior to finalizing the implementation. The technicians completing the installation activity will perform a walk-through with the Department Team to review deployment results, all installation documentation and checklists. Our Project Management Team will host a Customer Acceptance Review Meeting with the Department Team prior to finalizing the acceptance and cut-over at each location. During this time, we will

provide the Department with complete cable counts, station numbers and the required “as-built” drawings.

Installation Personnel

The CenturyLink Team warrants that all personnel providing installation of the OTS are direct Securus employees who have been fully trained and certified and are qualified to install the system, equipment and related services as required for service delivery.

As the incumbent provider, we will retain all existing support personnel. Each of these team members are qualified, fully trained and certified to deliver required services. Over the life of the existing contract, Securus has needed to backfill personnel. Each new employee will be fully trained and certified to deliver required services.

- 45. Proposer shall include, in detail, their Offender training program. Contractor shall describe how their approach will support that objective. (Section C.3.5.1, C.3.5.2, C.3.5.3)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The CenturyLink team has an extensive training staff, with curriculum tailored to the specific needs of user groups (e.g. administrative staff vs. investigations). While we have performed extensive training with Department staff on the existing system, this new contract provides an opportunity for re-training in addition to the more focused training needed for new services such as video visitation. As we have done in the past, the training plan will be developed in concert with TDCJ OTS administration and tailored to the Department’s needs.

Experienced CenturyLink Team employees conduct all training through on-site or online instructor-led classes, one-on-one and classroom training sessions at no cost. We deliver standard training using both hands-on experiences with your data and using instructor demonstrations to ensure each trainee understands all SCP functions.

Hands-on training is conducted by experienced CenturyLink Team employees. Our training programs enable facility staff to use all features the first day of installation. Since our products are web-based, after a two or three-hour training session, most facility staff can easily maneuver through the system’s features.

Department administrators are free to opt out of training if it is believed that your staff is up to date on the features of the OTS system. However, for your information, below are the available training modules for the current OTS.

SCP Course Modules

Course Module	Objective
Getting Started	<ul style="list-style-type: none"> • Logging in • Navigating through the features • Managing your password • Contacting Technical Support for service calls\

User Administration Activities	<ul style="list-style-type: none"> • Creating and changing user accounts • Defining a user's role and granting access permission • Resetting a user's password • Deactivating and/or deleting users • Running user management reports
Offender Administration Activities	<ul style="list-style-type: none"> • Adding and changing offender phone accounts • Deactivating offender phone accounts • Setting up the phones to meet your requirements • Using administrative reports
Monitoring Activities	<ul style="list-style-type: none"> • Reviewing Call Detail Records (CDRs) • Monitoring live calls • Listening to recorded calls • Using monitoring reports • Saving calls and burning to CD
Investigation Activities	<ul style="list-style-type: none"> • Using CDRs for investigations • Recognizing trends in offender activity • Using other investigative tools to collect evidence • "Digging" into the details
Super User Activities	<ul style="list-style-type: none"> • Learning time-saving tips and tricks • Discussing actual facility situations and turning evidence into intelligence • Troubleshooting for operational and maintenance staff to minimize unnecessary service calls

The following table presents the standard SVV training course modules and associated learning objectives.

Video Visitation Course Modules

Course Modules	Objective
Overview and Navigation	<ul style="list-style-type: none"> ▪ User types ▪ Appointment types ▪ Process flow ▪ URL - status bar - webcam ▪ Internet speed - storage term ▪ Three main modules
Appointments	<ul style="list-style-type: none"> ▪ Stop or cancel a session ▪ Change date/time ▪ Change terminal ▪ Live monitor sessions

- Administration**
- Session Viewer**
- Visitation Schedule**
- Optional Applications**
- Overview and Navigation**

- Users and user groups
- Terminals and locations
- Logs
- View a recorded session
- Actions and icons - search, play, lock, delete
- Customized by user type
- Sick Call - symptoms
- Commissary Ordering
- Automated inmate information
- User types
- Appointment types
- Process flow
- URL - status bar - webcam
- Internet speed - storage term
- Three main modules

We also offer customized training classes focused on different agency functions such as investigations, live call monitoring, and system administration.

User Manuals and Training Materials

We will provide all necessary user manuals and training materials to the Department staff at our instructor led training sessions. The training materials will be provided at no cost.

For SCP, we provide all user manuals, operating manuals, technical manuals and other instructions online. When an authorized user is logged into their SCP account they will see a “HELP” button in the upper right corner of the page.

SECURUS Technologies™

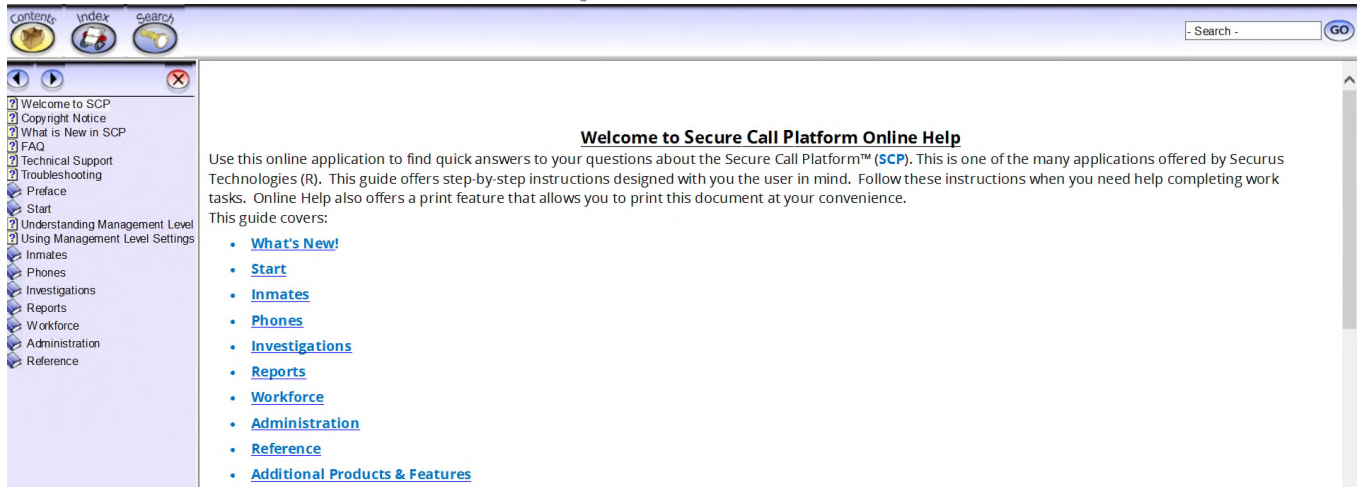
egallegos@SECUR.TX | Help | Log Out 
 Facility Routing Number: **99001**

Secure Call Platform

[HOME](#) | [SYSTEM](#) | [MONITOR](#) | [TOOLS](#) | [ADMIN](#) | [FACILITY PORTAL](#)

By clicking on this button another window will pop up for the Secure Call Platform Online Help.

Online Help Home Screen



Welcome to Secure Call Platform Online Help

Use this online application to find quick answers to your questions about the Secure Call Platform™ (SCP). This is one of the many applications offered by Securus Technologies (R). This guide offers step-by-step instructions designed with you the user in mind. Follow these instructions when you need help completing work tasks. Online Help also offers a print feature that allows you to print this document at your convenience.

This guide covers:

- [What's New!](#)
- [Start](#)
- [Inmates](#)
- [Phones](#)
- [Investigations](#)
- [Reports](#)
- [Workforce](#)
- [Administration](#)
- [Reference](#)
- [Additional Products & Features](#)

This is where manuals, instructions, and other information about SCP are located. TDCJ personnel will have the ability to search through the manual by Content sections, Index, or a general key word search function and print sections as needed. This method of “print what you need when you need it” ensures all printed material is updated with the current released product.

In this portal there is also an online self-help system available at all times from a handy Help menu in the application. Help Menu features include:

- Welcome Pages – Provides high level descriptions of the purpose and function of the selected feature.
- How To – Offers task based procedures to assist users in efficiently using the application to get their job done. Each topic includes a link to email Technical Support or Training for further assistance when necessary.
- What's New – Describes new features in the current release with links to more details or task based instructions.
- Related Topics – Links to similar topics users may find beneficial.
- Pop-up Definitions – Defines Glossary Terms and Index words at the click of a mouse without having to leave the topic to assist your users in quickly assimilating new concepts and technology.
- Tips and Tricks – Provides short cuts, helpful hints, and advanced topics for highly skilled users looking to improve their performance.
- Frequently Asked Questions (FAQ) – Offers common questions and their answers.
- Troubleshooting – Presents self-help to assist your users figure out unexpected results and what to do next to get back on track.
- Reference – Provides handy reference material such as international dialing codes and other resources for your user's convenience.

During training job aid handouts will also be distributed. Examples of handout topics include:

- SCP Call Restrictions with Call Type Descriptions
- Using Covert Alerts
- Reports – CDR Search Fields Descriptions
- Reports – Blocked Call Reasons Descriptions
- Reports – Call Termination Reasons
- Four Steps to Burn Call Recordings to a Disc
- Options for Burning Call Recordings to a CD
- Security Template Definitions and User Access Roles

Offender Training

Training begins during the voice biometric enrollment where the CenturyLink Team site administrators enroll the offender and explain to him/her the procedures for placing OTS calls. Following enrollment, procedures are reinforced in a number of different ways.

For traditional voice calls:

- Guided prompts to instruct offenders on OTS usage when they pick up the phone
- Educational Offender brochures in the intake packet.

HOW MUCH ARE THE CALLS <small>Rates (additional fees may apply)</small>	COMMON PHONE RESPONSES	COMMON PHONE RESPONSES <small>(continued)</small>	OFFENDER TELEPHONE SYSTEM (OTS)									
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Account Type</th> <th style="text-align: left;">Calls in Texas (per minute)</th> <th style="text-align: left;">Calls outside Texas (per minute)</th> </tr> </thead> <tbody> <tr> <td>Family and Friends Ac- counts</td> <td>\$0.26</td> <td>\$0.25 (Direct Bill) \$0.21 (F&F Prepaid)</td> </tr> <tr> <td>Offender Tele- phone Account</td> <td>\$0.23</td> <td>\$0.21</td> </tr> </tbody> </table> <p>REFUNDS - Released Offenders</p> <ul style="list-style-type: none"> • Upon release from incarceration an offender may request a refund of any funds remaining in his/her Offender Telephone Account. • The Texas Offender Telephone Account Refund Request form is available upon release or once released from the following website: www.TexasPrisonPhone.com. • Requests for refunds will be processed no sooner than 90 days after release and must be made within 12 months of release. • There is a \$3.50 processing fee. 	Account Type	Calls in Texas (per minute)	Calls outside Texas (per minute)	Family and Friends Ac- counts	\$0.26	\$0.25 (Direct Bill) \$0.21 (F&F Prepaid)	Offender Tele- phone Account	\$0.23	\$0.21	<p>"This number is not authorized."</p> <p>The number you dialed has not been successfully registered for you to call. Notify the owner of the telephone number that they must register their number at www.TexasPrisonPhone.com or 866-806-7804. Send a mail insert (available from offender telephone company representatives) which provides the instructions the family and friends must follow to register to accept phone calls from you.</p> <hr/> <p>"Your enrollment does not exist."</p> <p>Your voice is not enrolled in the system. Complete an OTS Assistance Request Form asking to be enrolled and put it in the mail box. An offender telephone company representative will arrive to enroll your voice.</p> <hr/> <p>"That is not a valid TDCJ ID number."</p> <p>The ID number you entered is not valid. The phones need a full 8 digit TDCJ ID number. If your number is less than 8 digits, you must enter leading zeros in front of it. Example: If your number is 123456, enter 00123456 to make a call.</p> <hr/> <p>"Your call was answered, but positive acceptance was not received from the called party. Possibly indicating an answering machine."</p> <p>The call could not go through because no one accepted the call.</p>	<p>"Your account has been suspended. Please try your call again later."</p> <p>You are on suspension or in transient status. When your status is cleared, the phones will allow you to make calls again. Offender telephone company representatives are not able to answer questions about suspensions.</p> <hr/> <p>"I am sorry; I did not recognize your voice." OR "I am sorry your verification failed."</p> <p>You are not saying your name the same as when you enrolled. If it continues, complete an OTS Assistance Request Form asking to be re-enrolled and put it in the mail box. An offender telephone company representative will arrive to reenroll your voice.</p> <hr/> <p>"You do not have sufficient funds to continue this call. Please hang up, and try your call again at a later time."</p> <p>The call could not go through because there is not enough funds in your Offender Telephone Account.</p> <hr/> <p>"That number is restricted."</p> <p>The restriction is on the owner of the telephone number not the offender. The owner of the telephone number needs to contact Securus Correctional Billing Services at 800-844-6591.</p>	<p>ELIGIBILITY</p> <p>Offender access to the OTS shall be validated and initiated by the telecommunications contractor based on the following eligibility requirements:</p> <ul style="list-style-type: none"> • Offenders classified as general population Levels 1, 2, 3, or 4 or protective custody Level 1 shall be authorized to access the OTS. • Offenders in a psychiatric inpatient program or Developmental Disabilities Program shall be allowed access to the OTS in accordance with the offender's treatment plan. • Eligible offenders in the infirmary shall have access to the OTS. <p>INELIGIBILITY</p> <ul style="list-style-type: none"> • Offenders in transient status, prehearing detention, solitary confinement, cell restriction, or special cell restriction shall not be permitted access to the OTS, regardless of custody designation. • An offender's access to the OTS may be suspended if the offender is found guilty of a major disciplinary violation in accordance with the <i>TDCJ Disciplinary Rules and Procedures for Offenders</i>. <p>OPERATION</p> <ul style="list-style-type: none"> • The OTS shall be operational between the hours of 7:00am and 10:00pm, seven days per week, with the exception of court time or any time day-room privileges are suspended due to a unit emergency or lockdown. • Offenders shall be permitted to call only landline telephone and post-paid cell phone numbers within the continental United States and Hawaii. • All telephone calls placed using the OTS shall be subject to monitoring and recording, except calls to the offender's attorney(s) of record. • An offender shall not be required to reenroll in the OTS when transferred to a new unit of assignment. <p style="text-align: right; font-size: small;">October 13, 2014 TX011</p>
Account Type	Calls in Texas (per minute)	Calls outside Texas (per minute)										
Family and Friends Ac- counts	\$0.26	\$0.25 (Direct Bill) \$0.21 (F&F Prepaid)										
Offender Tele- phone Account	\$0.23	\$0.21										

<p>GUIDELINES</p> <p>Offenders shall conduct telephone conversations in an acceptable manner. Loud, boisterous conversations shall not be permitted. Offenders are prohibited from speaking in code, passing gang related information, planning criminal activity, or using the telephone in furtherance of criminal conduct. Threats, obscenities, and other types of abusive language may result in immediate termination of the telephone call, suspension of future telephone privileges, and disciplinary action.</p> <p>Unauthorized contact with a victim or a member of a victim's family by an offender is prohibited in accordance with AD-04.82, "Forfeiture of Good Conduct Time for Contacting a Victim Without Authorization."</p> <p>The following types of calls and conversations will not be permitted: calls to pre-paid cell phones; calls to businesses; international calls; forwarded calls; three-way calls; conversations with any adult not on the Approved Calling List; conversations where a speakerphone is being used.</p>	<p>FAMILY and FRIENDS MUST REGISTER TO RECEIVE YOUR CALLS -</p> <p>They can register a landline by going to the following website: www.TexasPrisonPhone.com or calling (866) 806-7804.</p> <p>They can register a Post-Paid cell phone at www.TexasPrisonPhone.com/cellphone.asp or by calling (866) 806-7804 and selecting options 1, 0 and following the prompts.</p> <p>In order to receive calls from an offender, the Texas Department of Criminal Justice requires that your family and friends register and meet the following requirements:</p>	<p>WHEN YOU MAKE A CALL</p> <ol style="list-style-type: none"> 1. Pick up the handset; choose 1 for English or 2 for Spanish and follow the prompts. 2. Press 1 for Collect Call or 2 for Debit Call. 3. Enter your TDCJ ID #. (Enter all eight digits, including any zeroes at the beginning of your TDCJ ID number. For example: 00123456). 4. Enter the telephone number. Telephone number validation occurs. 5. Say your name exactly as you said it during enrollment. Say "Texas Department of Criminal Justice". Voice recognition occurs. 6. You will be connected to the called party. 	<p>PAYING FOR YOUR CALLS</p> <p>There are three payment options:</p> <p>COLLECT CALL (DIRECT BILL) – The person you call accepts the charges when you call them. A Direct Bill account for collect calls is automatically created for your family and friends when they were approved to receive calls. The account will have an initial credit limit of \$85 which will be increased to \$200 after 90 days if the account is kept current and your family and friends have paid the invoice in full and on time. The offender will place a collect call and family and friends accept the charges. Family and friends receive a monthly invoice. If your family and friends reach their credit limit prior to the next bill cycle, and have not made a payment on the account the phone number is blocked. They need to simply contact Securus Conventional Billing Services (SCBS) 800-844-6691 and make a payment and the line will be unblocked and ready to receive calls.</p> <p>If a Direct Bill account becomes past due, it is automatically converted to a Friends and Family Prepaid account.</p>
<p>OFFENDERS MUST ENROLL YOUR VOICE - Voice Biometrics validates "you are who you say you are" before connecting a call. Your enrollment is supervised by an offender telephone company representative. If you do not cooperate with the process, you will not have phone privileges. To enroll:</p> <ol style="list-style-type: none"> 1. The enrollment representative matches your TDCJ identification card to the enrollment list. 2. Pick up the handset and enter your TDCJ number (PIN). (Enter all eight digits.) 3. Follow the prompts and repeat your first and last name four or more times until it is verified. SPEAK LOUDLY, CLEARLY, and SLOWLY 4. When prompted for the facility name, say - TEXAS DEPARTMENT OF CRIMINAL JUSTICE four or more times until it is verified. <p>5. Return the handset to the phone cradle.</p> <p>NOTIFY YOUR FAMILY and FRIENDS - Send a mail insert (available from offender telephone company representatives) which provides the instructions the family and friends must follow to register to accept phone calls from you.</p>	<ol style="list-style-type: none"> 1. The name on the telephone service bill/listing must match the name on the registrant's driver's license or state identification card. 2. Family and friends must agree to the following conditions: <ul style="list-style-type: none"> • Family and friends are the registered owner of the phone that will receive calls from the offender • Family and friends will allow offender calls to their phone • Family and friends are at least 18 years old • Family and friends will not forward calls, make 3-way calls, or use a speakerphone on calls received from the offender <p>How do offenders know when their family and friends are registered to receive telephone calls from them?</p> <p>At any time an offender, through a menu option (choose 9) available on the offender telephones, can listen to a list of the family and friend telephone numbers that have been registered to receive calls from the offender.</p>	<p>WHEN YOUR FAMILY and FRIENDS ACCEPT THE CALL FROM YOU</p> <p>ANSWERING A CALL - When family and friends answer a call from TDCJ, remember... A computerized voice will tell them the call is from TDCJ and ask them to respond to a few questions.</p> <p>AVOID BEING DISCONNECTED - If family and friends do any of the following during the call, they could be disconnected:</p> <p>DO NOT...</p> <ul style="list-style-type: none"> Transfer the call (you cannot transfer or forward a call between your registered landline and your registered cell phone) Use call waiting or call forwarding Put the call on hold Press any button on the key pad Conference another person on the phone Attempt to make a 3-way call Use a speakerphone 	<p>FRIENDS and FAMILY (F&F) PREPAID - After your family and friends telephone number is registered and validated, the person who owns the number can fund their own prepaid account so they can receive calls. A prepaid account ensures your family and friends are always ready to receive your calls. Since your family and friends pay before being called, there is never a disruption in service. Family and friends can request their Direct Bill account be converted to a prepaid account at any time.</p> <p>OFFENDER TELEPHONE ACCOUNT - When you enroll your voice in the phone system an Offender Telephone Account is automatically created for you. Anyone can add money to your Offender Telephone Account. You can fund your own account too. You can purchase phone time in any dollar amount using funds from your Trust Fund Account. Sales tax is charged on the purchase and sales are final. An offender may request to move funds from his/her Offender Telephone Account to his/her Trust Fund account by submitting an OTS Assistance Request Form. There is a \$3.50 processing fee and processing can take up to fifteen (15) calendar days.</p> <p>Funds placed in an Offender Telephone Account become the property of the offender and can be used by the offender to call anyone on his/her Approved Calling List. Family and friends will not be able to receive refunds from this account.</p>

- We work with UTMB staff to train hearing impaired offenders on VRS
- Videos located on the terminal for hearing impaired – There are currently three available videos that were all custom produced for TDCJ by the Century Link Team: 1) ASL VRS tutorial, 2) ASL VRS rules video, 3) OTS rules.
- Printed Instructions –Durable printed dialing instructions are located at each offender telephone location in English, Spanish, and the other languages specified by the Department. 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. All offender telephone placards include a warning that calls may be monitored and recorded. In addition to the placards, an admonishment will be played during every call informing both parties that this call may be monitored and recorded (except attorney calls).

CenturyLink Public Communications, Inc.
This call is subject to being monitored and recorded.

Press '1' for English.	Enter area code and phone number.
Marque '2' para Español.	Marque su numero de telefono, incluya su codigo local o lada.
For a collect call press '1'.	Say your full name to verify your voice.
Para llamada a cobarse, marque '1'	Diga su nombre completo para verificar su voz.
For a debit call press '2'.	You may hear silence during the acceptance of your call. Please continue to hold.
Para llamada por débito, marque '2'.	Vas a oír silencio mientras aceptan su llamada.
Enter your PIN Number.	Continue esperando por favor.
Marque su numero de identification personal.	

- The CenturyLink Team offers to produce short instructional videos for intake or other areas if desired by the Department

For Video Visitation TDCJ Specified Locations

- The CenturyLink Team will create and produce an educational brochure about video visitation, similar to the OTS insert, which can be included in the intake packet for offenders at the 6 sites that will have video visitation.
- Our video visitation application is very intuitive and will provide the offender with guided prompts to instruct on usage.

*e-messaging is an in-bound service only with messages being printed and distributed to the offender like regular mail. In the future if two-way messaging is desired by the department, all training materials and brochures will be provided to the offender.

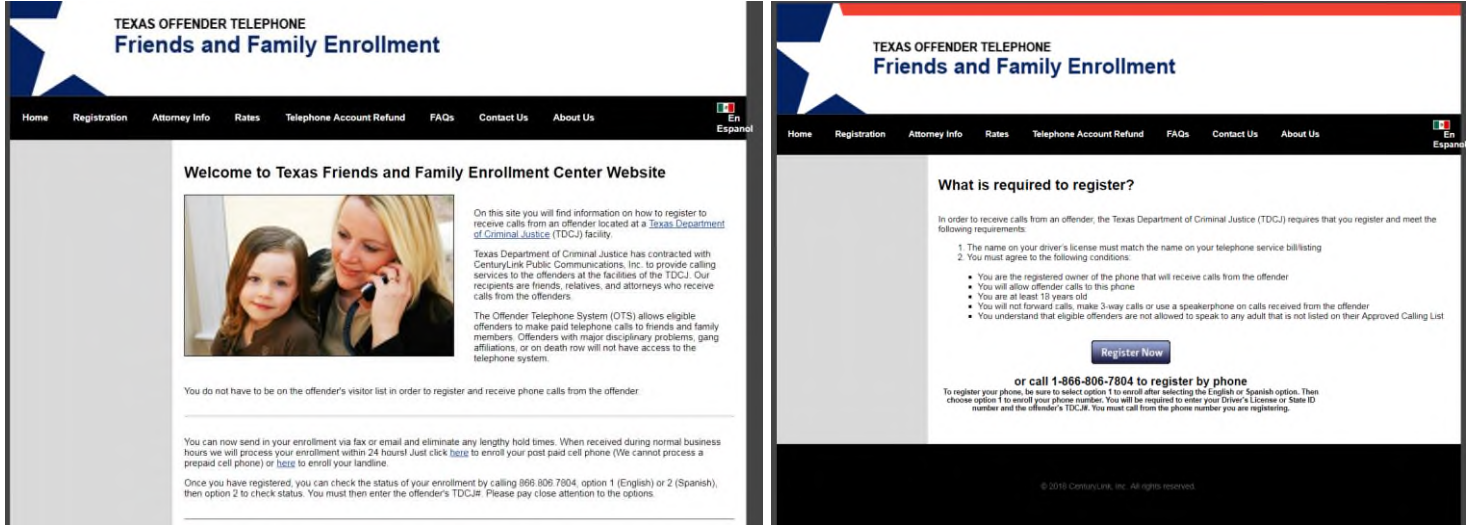
CALLED PARTY TRAINING

Friends and Family have multiple options available to them on explaining telephone system usage, account management, and rates.

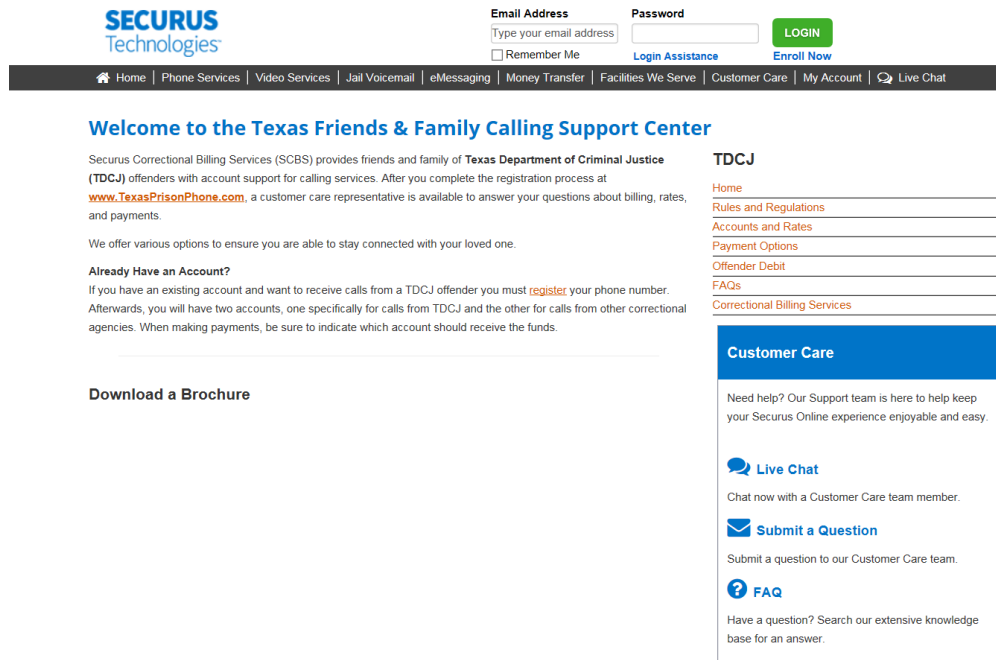
Training Materials

- **Mail Insert** – Each offender is given a handout in their intake packet that they can mail to Friends and Family with their PIN number and instructions on how to register to receive calls. We will also provide an insert about video visitation for offenders at the specified video visitation sites that can mailed to friends and family.
- **TDCJ Friends and Family Websites:** Both of these easy to use websites were created specifically for TDCJ. They both include includes rates, fees, policies, registration requirements, ways to contact the CenturyLink Team, and answers to frequently asked questions.

- www.texasprisonphone.com: This is the Texas Offender Telephone Friends and Family Enrollment website. After initial enrollment with a representative, Friends and family are walked through the next steps and informed on the status of their final enrollment.



- securustech.net/tdcj : This is the Texas Friends and Family Support website for Correctional Billing Services. From this website Friends and Family can add funds to their account, access Rules and Regulations, read FAQs, submit a question or chat with a representative. Educational brochures are also available for download.



TDCJ Frequently Asked Questions

How much does a call cost?

Rates vary depending upon if you live in or outside of Texas. For specific rates, [click here](#).

When will I get my first call?

Unfortunately there is no easy answer. There are three main steps:

1. Your name must match your driver's license or State ID and your phone bill.
2. You must register and be approved to receive calls.
3. The offender enrolls in the voice biometrics system and is eligible to make calls. The whole process can take 7-30 days depending on timing and resource availability.

I was approved to receive calls, but I have not received any. Why?

There are a number of reasons this may be occurring. Some include:

- the unit was on lockdown when he/she wanted to call you
- no one was home to press # 1 and accept the call. (Offenders cannot leave voice messages)

Can I add money to an Offender's Debit Account?

Yes you can! For details [click here](#).

My offender says that when he calls me the recording says my phone is restricted, why?

There are a couple of possibilities:

- The registration process may not be complete, to verify call 866 - 806 - 7804 (use option 1, 2, 0, 0) or visit website www.texasprisonphone.com/contact.asp.
- There may be an issue with your billing account, to verify call 800 - 844 - 6591 or [click here](#).

TDCJ

- [Home](#)
- [Rules and Regulations](#)
- [Accounts and Rates](#)
- [Payment Options](#)
- [Offender Debit](#)
- [FAQs](#)
- [Correctional Billing Services](#)

Customer Care

Need help? Our Support team is here to help keep your Securus Online experience enjoyable and easy.

 [Live Chat](#)

Chat now with a Customer Care team member.

 [Submit a Question](#)

Submit a question to our Customer Care team.

 [FAQ](#)

Have a question? Search our extensive knowledge base for an answer.

***All training materials are available in English and Spanish**

Friends and Family Customer Service

Live agent support is available to friends and family members from an in-sourced, US-based call center seven days a week, 24 hours a day, and 365 days a year.

Customers can use our toll-free number (1-800-844-6591) to either speak to a live agent or use an intuitive, automated interactive voice response system to help them with their needs. End-users can also now access Securus customer service via online "chat" 24 hours a day, seven days a week.

Our friendly and knowledgeable agents can help customers with:

- Setting up and funding accounts
- Making payment arrangements
- Obtaining information on credit limits
- Resolving complaints
- Blocking and unblocking numbers
- Reviewing call durations and history
- Learning about MoneyGram® options
- Learning about Western Union® options
- Receiving information on new services
- Confirming originating facility

- Reviewing account balances
- Answering questions and helping customers with refund requests
- Managing account notifications

Our customer service agents are highly trained on OTS issues and in satisfying the specific needs of called parties. We offer both English speaking and Spanish speaking agents.

Post-System Initiation Training

The CenturyLink Team will have available training personnel available for retraining and consultation. The available personnel will be experienced trainers, not service technicians.

- 46. Proposer shall include a toll free single dispatch telephone number and e-mail address for placement of service calls 24 hours a day, 7 days a week. (Section C.3.6)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

As we have done for the past 9 years, the CenturyLink Team will be solely responsible for trouble shooting problems and providing all service and maintenance to the entire OTS system, including meeting and exceeding all J.4 Contract Performance Measures. We have an already established and implemented toll free single dispatch telephone number and email address for the Department and the support team to ensure prompt problem resolution for any service calls we receive from TDCJ. To handle any service requests, the CenturyLink Team created and staffed a dedicated TDCJ Technical Support Center (TDCJ-TSC) in the Securus headquarters in Dallas, TX. The TDCJ-TSC is available 24 hours a day, 7 days a week, 365 days per year and can be contacted via one of the following methods:

Our TDCJ-TSC has maintained a well <30 second Average Speed of Answer over the last 9+ years.

- Phone: 866-206-7151
- Email: tdcjsupport@securustech.net

- 47. Proposer shall describe service procedures from the point of discovery and reporting to problem resolution. Proposer shall provide a copy of service escalation procedures complete with names and telephone numbers of persons to be notified. Support up to and including manufacturer warranty support should be included. (Section C.3.6)**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The CenturyLink Team acknowledges that the OTS and eMessaging systems provide the Department with a revenue stream and must remain in good working order. We have worked hard developing a redundant OTS system that is proactively monitored so that no problems arise. However if any of the system failures occurs as listed in Exhibit J.4 – Contract Performance Measures, our team can restore to full capacity within the required time frame.

System Redundancy, Fault Tolerance and Monitoring

Redundancy is a key component of the Secure Call Platform (SCP). While operating on a single platform, 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 CenturyLink Team will coordinate with the Department an approved system outage for an annual failover test, and within two weeks of that test provide adequate test results to demonstrate success.

Proactive Monitoring

Data Centers and Network

We continuously monitor all data centers, infrastructure components, platform systems and Offender Telephone Systems (OTS) 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.

Premise Equipment

The dedicated TDCJ Technical Support team provides 24x7x365 monitoring of all facility-based equipment and directly supports facility installations via telephone and email. Technical Support monitors connectivity for all installations and all installed equipment including Integrated Access Devices (IADs), Visitation Phone Monitoring (VPM) units, switches and Uninterrupted Power Supply (UPS) systems. The systems are polled every two minutes and their vital operating statistics sent every 10 minutes. Upon receiving an alert indicating network failure, The TDCJ Tech Support will open a trouble ticket with the appropriate circuit provider. In the case of a premise-based equipment failure, a Field Technician is dispatched to the facility for on-site repair.

In addition to real-time monitoring and alerting, Securus Technical Support also leverages the SolarWinds® network performance monitor to gather and evaluate historical data for network alerts, bandwidth usage, packet loss and hardware performance. The detailed level of monitoring available via our network performance monitor allows the Technical Support group to take proactive steps to prevent or mitigate facility outages and to ensure the correct resources are engaged if dispatch is necessary.

Through network monitoring Securus can:

- **Proactively repair systems to prevent outages.** Many times corrections are made before a facility is aware of a problem. This means less downtime and increased system reliability for the facility.
- **Alert remote or on-site engineers of system threshold inconsistencies or alarms.** The NOC communicates with engineers through e-mail, short message service (SMS), or directly through a wireless phone to address the issue.
- **Receive real-time alerts when the system detects an error.** Monitoring identifies if network elements exceeded established thresholds and alerts Securus personnel of possible carrier network issues.
- **Ensure sufficient resources are in place.** The Securus capacity engineering team reviews call traffic volume reports and storage requirements throughout all systems to ensure sufficient network capacity.

Service Response Times and Escalations

The CenturyLink Team maintains a center with personnel dedicated to TDCJ. These personnel are comprised of the Technical Support Manager, Technical Support Supervisor, 6 Data Administrators, and 18 Service Representatives.

Upon point of discovery or receiving a trouble report from TDCJ staff our personnel will begin to resolve the issue following the prescribed service policies in place to insure that the system is operating at its full capacity at all times. Our established service procedures lay out response times and service levels that accomplish our objective of providing exceptional customer service and adhering to the Department's requirements in J.4.

Our dedicated TDCJ Technical Support Center has a 99.9% SLA compliance

A trouble ticket will be generated and assigned a tracking number and an initial acuity level. The acuity of each ticket is escalated one level when we do not meet the established time requirements for that acuity level.

The following provides an overview of the CenturyLink Team policy for internal response to incoming trouble reports:

- STEP 1:** The TDCJ Technical Support Center (TDCJ-TSC) becomes aware of the issue either through proactive monitoring or through the Department calling the TDCJ dedicated toll free number or e-mail. The ticket is created by the Service Representative who identifies the caller and site location and enters the information in the database.
- STEP 2** The nature of the issue will determine the course of action taken by the Service Representative:
- a. If the issue is software related, the Service Representative will begin initial troubleshooting/research to diagnose and resolve the issue.
 - b. If the issue is hardware in nature, or the Service Representative is unable to remotely diagnose the issue the ticket will be escalated to a Data Administrator.

- c. The Data Administrator will determine if a field service technician needs to be dispatched to resolve the issue.
- d. If it is a network issue, then the Network Operations Department personnel will become actively involved.

STEP 3 If a field service technician was deployed, they will be responsible for resolving the issue or will contact the TDCJ Technical Support Center for further direction.

STEP 4 If the problem remains unresolved, the Data Administrator contacts the TDCJ-TSC Technical Support Manager for further direction in resolving the problem. If necessary, a Senior Technician will be dispatched to further assist.

STEP 5 Problem resolved and tested. The Data Administrator retains accountability for the ticket until it is resolved and confirms resolution with the Department.

ESCALATION POLICY

Each service issue is assigned one of three initial acuity levels, each with its own resolution and escalation timelines. Every effort is made to resolve the problem remotely, within the framework of the resolution timeframes. If the problem cannot be resolved remotely, a service technician is dispatched to the facility to expedite problem resolution. Technician dispatch also has resolution and escalation timelines appropriate for the assigned acuity level.

If resolution is delayed, escalation procedures within CenturyLink Management Team are activated to ensure appropriate resources are allocated to resolve the problem.

Service Response Times and Escalations

Priority Level	Service Priority Description	Resolution Time	Customer Communication Guideline	Escalations
P1	A P1 is our highest service level defined as 20% or more of the functionality of the System being adversely affected by the System Event. Examples of P1 service assignments would include items such as no voice prompts, features not operating appropriately, issues with listening to live calls, inability to access SCP UI, all phones down.	6 hours	<ul style="list-style-type: none"> • Technical Support Center notifies the facility when the service issue is resolved • If a field technician is required onsite, the Data Administrator contacts the 	<ul style="list-style-type: none"> • If resolution is delayed, escalation procedures within the Management Team are activated to ensure appropriate resources are allocated to resolve the service request • Technical Support Manager & Field Service Manager • Technical Support

			customer with an estimated time of arrival	Director & Field Service Director <ul style="list-style-type: none"> VP Service & Operations
P2	A P2 assignment defined as less than 20% greater than 10% of the functionality of the System being adversely affected by the System Event. This would also include inoperative workstations.	24 hours	<ul style="list-style-type: none"> Technical Support Center notifies the facility when the service issue is resolved If a field technician is required, the Data Administrator contacts the customer with an estimated time of arrival 	<ul style="list-style-type: none"> If response is delayed, escalation procedures within Securus' Management Team are activated to ensure appropriate resources are allocated to resolve the service request Technical Support Manager & Field Service Manager Technical Support Director & Field Service Director VP Service & Operations
P3	A P3 assignment defined as less the 10% of the functionality of the System being adversely affected by the System Event. Single and multiple phones related issues. Examples of P3 service assignments would include items such as static on the phone, a party not being able to hear, unable to dial, a broken phone, dial pad not working, and inability to generate reports.	72 hours	<ul style="list-style-type: none"> Technical Support Center notifies the facility when the service issue is resolved If a field technician is required, the Data Administrator contacts the customer with an estimated time of arrival 	<ul style="list-style-type: none"> If response is delayed, escalation procedures within Securus' Management Team are activated to ensure appropriate resources are allocated to resolve the service request Technical Support Manager & Field Service Manager Technical Support Director & Field Service Director VP Service & Operations

Escalation Contacts:

Technical Support (All Levels)		
Acuity Level	Contact	Telephone Number
Level 1	Manager Tony Taillac	Work: (214) 775-2702 Cell: (214) 727-5376
Level 2	Director Terrance Clair	(936) 355-3306
Level 3	VP of National Operations Barry Brinker	(503) 990-6466
Level 4	VP/GM Paul Cooper	(720) 264-8121

48. Proposer shall provide a Quality Control Plan for monitoring and assessing the success of its service. (Section C.3.8)

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY

The CenturyLink Team manages a rigorous quality control plan to monitor and assess the success of its services for TDCJ. A copy of our complete Quality Control Plan can be found in Attachment G – Quality Control Plan. On a regularly scheduled basis the CenturyLink Team currently provides the following required reporting to Department staff. The frequency and delivery of this reporting will continue to be in compliance with all required content and delivery timeframes under the new contract.

Report	Description	Frequency
Approved Calling List Audit	Re-Verification of Existing PANs	Monthly
Friends and Family Offender Requests for Assistance Log	Dispositions of requests received by TDCJ OTS office	Monthly
Friends and Family Enrollment Report	Phone numbers approved and not approved	Monthly
Land Lines Ported to a Cell/Blocked Report	Phone numbers converted from landline to cellphone	Monthly
Monthly Statistical Report	Key metrics for calls, tickets, eMessaging	Monthly
New Attorney Report	Newly enrolled attorneys	Monthly

Report	Description	Frequency
Offender Calling Pattern (Top 100 Offenders)	Offenders with the highest number of call minutes	Monthly
Supervised Enrollment Report	Offenders enrolled and re-enrolled in voice biometrics	Monthly
Vacancy Report (Wireless Containment System)	Contractors who are assigned to the project	Monthly
Vacancy Report (OTS System)	Contractors and vacancies who support OTS	Monthly
Bandwidth Report	Key metrics for network utilization	Monthly
Network Spikes	Network utilization above a predefined percentage	Monthly
One to Ten Days – Over 1000 Minutes	Call activity in the first ten days	Monthly
Service Ticket Report (OTS)	Service tickets by priority levels	Monthly
TDCJ Commissary Refunds Report	Offenders who have requested phone refunds during incarceration	Monthly
TDCJ Released Offender Telephone Account Requested Refund Report	Offenders who have requested phone refunds after prison release	Monthly
Commission Report (eMessaging)	Revenue and commissions for eMessages	Monthly
Commission Report (OTS)	Revenue and commissions for completed calls	Monthly
Lockdown Days	Days when phones are unavailable	Monthly
Phones Used at Maximum Level 5-10 PM	Call metrics during peak utilization times	Monthly

Report	Description	Frequency
Monthly Presentation Report	Charts and graphs of key OTS and related metrics	Monthly
PM Report	Results of inspection of phones and OTS equipment	Monthly
Top 10 Number Called Agency-wide	Phone numbers receiving the highest number of calls	Monthly
Active PAN Report	Current approved phone numbers	Three times a month
Consumables Report	Printer supplies purchased	Quarterly
Installation and Activation of Additional Work Stations	New workstations installed	Quarterly
Attorney Quarterly Audit	Re-verification of enrolled attorneys	Quarterly
Network Redundancy Testing Report	Results of failover testing between two independent data centers	Twice Annually
Correctional Billing Service Quality Metrics	Key metrics of number and length of customer calls	Monthly
TDCJ Customer Satisfaction Survey	Key metrics related to customer response on service and offerings	Annually

49. Proposer shall propose additional services that may have added value to the Department. (Section C.3. 10)

The CenturyLink Team is proposing Added Value Services that are directly related to the OTS. All Added Value Services and features that are agreed to will be provided at no cost to the Department over the life of the contract.

CenturyLink understands that the Department will score call rates and at the same time evaluate and score the Added Value Services. Certain optional Added Value Services are included in the end user base rate per minute, while other optional Added Value Services contain a cost that is added to the end user base rate per minute.

Added Value – Option #1 - PREA Line

The Prison Rape Elimination Act (**PREA**) is a federal law, Public Law 108-79, signed into law in September 2003 by the President of the United States and now designated as 42 USC 15601. **PREA** establishes a zero-tolerance standard against sexual abuse of incarcerated persons of any age.

The Secure Call Platform (SCP) allows offenders to report PREA incidents to the facility via the ITS system.

Investigators have the ability to set up any phone, voice mailbox, or answering machine to answer calls from informants without any indication in the SCP call detail reports, global lists, or to other inmates. It is a completely anonymous call with all information hidden from normal investigator views. The CenturyLink Team will work with the Department to facilitate best practices in setting up this valuable tool.

Option #1 Cost = Included in base rate per minute

Added Value – Option #2 - Automated Information Services 2.0

The CenturyLink Team is proud to offer the Securus Automated Information Service (AIS) to allow TDCJ offenders the ability to securely access facility information and information specific to themselves from an automated interactive voice response (IVR) system. AIS is the industry's first and only hosted IVR service that provides general facility and offender-specific information to offenders and outside callers over the phone.

In addition to this core functionality, AIS can be configured to allow friends and family members to fund a pre-paid telephone account or an inmate trust account. TDCJ offenders can also use the AIS for automated inquiries such as obtaining their Trust Account balances over the phone. This functionality is available around the clock, which means offenders, friends & family will always be able to get the information they need when they are able to access it.

Family members and friends access AIS by calling a designated number, typically the facility's main telephone number. Offenders access the system through standard offender telephones, without the need for new hardware or wiring. Offenders call the AIS by dialing a speed dial number (generally *111). Finally, the Department staff will be able to re-focus their time and efforts on critical tasks and projects, since they won't be repeatedly answering the same offender-focused questions over and over.

AIS can be configured to provide:

- Trust Fund balances
- Visitation eligibility
- Account Funding
- Voicemail
- General facility information
- Frequently asked questions and responses

AIS retrieves information from the Department's management information systems to obtain Trust Account balances, visitation eligibility, voicemails and related data every 15 minutes. The service offers an English and Spanish interface, text-to-speech playback of offender names, and a touchtone or speech recognition interface. Additional AIS benefits include:

- Improved efficiency – quickly answering offenders, family members, and friends while freeing staff to focus on other responsibilities
- Use of phone system already installed – no need for additional hardware or wiring
- Significantly reduce questions answered by staff – AIS provides 24-hour access and eliminates most common questions
- Usage summary provided to the facility every month

Option #2 Cost = Included in base rate per minute

Added Value - Option #3 - Voicemail

The Voicemail service, similar to inbound email, is a one-way communication product that allows family members and friends to leave a 60-second voicemail for an offender. This provides a quick and easy way for the offender's loved ones to initiate communication or deliver timely information to an offender. When an offender calls into AIS, they will be alerted to a new voicemail message. As is the case with all offender telephone calls, our Voicemail is recorded and monitored for investigative purposes.

Additional Voicemail benefits include:

- Enables communication at times other than scheduled telephone calls
- Provided at no cost to the offender or facility (family pays the per minute rate)
- Ability to review and save messages for 60 days from the date it was created

Further, The CenturyLink Team has fully integrated our Voicemail product into the Secure Call Platform (SCP) to enhance investigative capabilities. SCP has the ability to ensure that Voicemail recordings are readily available to the offender and easily distinguished from other calls.

Option #3 Cost = Voicemail at a negotiable price per voicemail (CenturyLink proposes \$0.35 per voicemail) commissioned to the State at the mandated 40% rate.

Added Value – Option #4 – Contraband and Cell Phone Detection Devices

The CenturyLink Team is giving the Department the option of obtaining CellSense contraband and cell phone detection units. The CenturyLink Team will purchase a certain number of these devices on behalf of the Department. Once delivered, TDCJ will retain ownership of all equipment and warranties

CellSense

Cellsense detects contraband items containing ferrous metals through the use of ferromagnetic detection (FMDS) technology. Only ferrous metal objects that are in motion are detected.

Cellsense is the original and only contraband & cell phone detector designed for use by corrections departments to enhance their capabilities to detect and confiscate contraband.

Cellsense's one-of-a-kind versatility provides mobile inmate search at any location, indoors or outside. The unique single pole design and long-life battery extend its versatility for screening in all areas of the correctional facility.

Designed to eliminate complicated dials and controls, Cellsense can be operational for trained staff in 10 seconds. No calibration and minimal user input is needed for operation. An intuitive "stop light" visual alert system combined with audible alerts make detection easy for all staff.

- **Portable, full body screening for small and large size objects:** Full scan of the entire body in a single walk-by at high throughput (40 subjects per minute)
- **Versatile:** Functions in vertical and horizontal positions to screen inmates and their belongings
- **Covert screening:** Useful for surprise and covert screening of inmates and their belongings, including mattresses, laundry items, and commissary items
- **Detection of cell phones:** Detect cell phones when on or off, and anywhere on the person or internalized



- **Easy to deploy:** Setup and begin screening in 10 seconds
- **Safe & non-emitting:** Does not radiate or emit, making it 100% passive and safe for all individuals including those with pacemakers or who are pregnant

- **Ruggedized:** Designed to withstand harsh conditions and treatment, both indoors and outdoors
- **Behind-the-wall training included:** On-site training, both in classroom and behind the wall, provided by Metrasens certified trainers with 40 years' combined experience in prison security

Option #4 Cost = Add \$0.006 to base rate per minute for 100 CellSense Units

Added Value – Option #5 – ADA Compliant CapTel Phones

Captioned Telephone (or CapTel for short) is a new telephone technology that allows people to receive word -for-word captions of their telephone conversations. The CapTel phone looks and works like a traditional phone, with callers talking and listening to each other, but with one very significant difference: Captions are provided live for every phone call. The captions are displayed on the phone's built in screen so the user can read the words while listening to the voice of the other party.

Securus will provide Captel phones integrated with SCP to allow ADA/CapTel compliant hard of hearing inmates the ability to use these without TDCJ losing any security features / benefits that would be available on a standard SCP inmate phone.

Option #5 Cost = Included in base rate per minute

Added Value - Option #6 – Expansion of Video Visitation

The 12 units identified by TDCJ in this solicitation for the video visitation solution include:

Visitor Site	Offender Site
Houston - Jester III	Amarillo - Clements
Beeville - Garza Complex	Kennedy - Connelly
Dallas - Hutchins	Gatesville - Crain
Lubbock - Montford	Tennessee Colony - Michael
Austin - Travis	Beaumont - Stiles
El Paso - Sanchez	Huntsville - Wynne

The base rate per minute includes deployment of 10 video visitation stations at each of the 12 facilities, for a total of 120 visitation terminals.

As an extension of video visitation program, the CenturyLink proposal gives the Department the option to select other Offender and Visitor sites to allow for facility to facility visits.

For deployment of an additional 200 visitation terminals at 20 additional facilities, the following optional pricing would apply.

Option #6 Cost = Add \$0.005 to base rate per minute for 200 more offender visitation stations

Added Value - Option #7 – Expansion of Prison Entrepreneurship Program

As an extension of video visitation and in furtherance of the Department’s re-entry objectives, CenturyLink offers a comprehensive turnkey video conferencing solution for the Prison Entrepreneurship Program (PEP). The solution would connect PEP instructors in Dallas and Houston to offenders at up to 10 TDCJ facilities, with up to 200 simultaneous participants. In addition, each training session would be recorded and available to playback for up to 12 months.

The Prison Entrepreneurship Program (PEP) harnesses the entrepreneurial instincts of incarcerated men and women to transform their futures, their families and their communities. Since 2004, PEP has been on a mission to transform inmates and executives by unlocking God-given potential through entrepreneurial passion, education and mentoring. Our globally recognized “entrepreneurship boot camp” delivers the State’s best results in terms of improving employment and reducing recidivism.

Population served

PEP serves offenders in Texas, beginning up to three years prior to their release and continuing indefinitely post-release. This “inside-outside” strategy differentiates PEP and contributes significantly to its outstanding outcomes. About 60% of PEP’s participants were convicted of a violent crime and 40% have previously served time in prison; none is a convicted sex-offender. PEP has full service offices in Houston and Dallas, with re-entry support also provided in Austin. PEP operates three transition homes in Houston, two in Dallas and one in Austin with a combined capacity of 120 beds. About 50% of PEP graduates typically release to Houston, about 40% to Dallas and 10% to Austin or other areas.

PEP’s services begin inside the prison system with a rigorous application and screening process that (at current scale) selects only the top 1,200 applicants from a pool of about 15,000 eligible men and women. Selected participants are transferred by TDCJ to one of the prisons where PEP operates (currently four).

Program Elements

Phase 1: The Leadership Academy

Once transferred, participants begin with a 3-month, in-prison character development program, also known as the Leadership Academy (“LA”). This phase helps prepare participants for PEP’s core entrepreneurship curriculum – and for life post release. All participants are expected to study and “live out” PEP’s 10 Driving Values: Integrity, Accountability, Wise Stewardship, Love, Fun, Fresh-Start Outlook, Servant-Leader Mentality, Innovation, Execution and Excellence. PEP’s Leadership Academy is facilitated mostly by graduates from previous classes (called “Servant Leaders”), as well as PEP staff and volunteers.

Phase 2: Business Plan Competition

Immediately following the Leadership Academy, participants complete a 6-month, “mini MBA” program in prison. The foundation of PEP’s in-prison business education is the core curriculum taught by PEP staff, board members, and business executives (“Executive Volunteers”) lecturing on topics within their areas of expertise.

The centerpiece of this phase of PEP’s program is the Business Plan Competition (“BPC”), modeled after BPCs held at many major universities. Each student is required to conceive of a business that he / she would start upon release, research the feasibility of competing successfully within his / her chosen industry, write a complete business plan for launching his /

her business and then pitch this plan regularly in a “Shark Tank” format to panels of Executive Volunteers. During this phase, all students also complete and receive certificates for a financial literacy course, an employment workshop, a business etiquette course and a Toastmasters class. Over the duration of the course, each student receives extensive feedback from other volunteers, including college students, on his / her written plan through e-mail correspondence and a series of workshops held within the prison. The significance of the role of Executive Volunteers in this phase cannot be overstated.

Phase 3: Post Release Services

These in-prison services are followed by comprehensive post-release services. PEP provides its graduates with a structured environment of encouragement, support, and accountability. PEP’s transition services include, among other elements, intensive case management with a dedicated re-entry specialist; an affordable housing program that provides a secure, supportive environment to begin rebuilding a life; assistance with finding employment through a network of local businesses; a weekly continuing education program led by volunteer business leaders; and business start-up support services, including affordable incubation space, bookkeeping and access to PEP’s network as prospective customers for their businesses.

Program Results

Since 2004, PEP has considerably increased employment rates and business ownership for male ex-offenders (PEP began serving female offenders in late 2017) while dramatically reducing recidivism. PEP’s 1,500+ released male graduates have achieved the following results:

PEP Success Metrics		
CRITERIA	GOAL	ACTUAL
Employment	100% employed within 90 days of release	100% employed within 90 days of release; in 2017, PEP graduates averaged only 24 days “from prison to paycheck”
Starting Wage	125% of minimum wage (\$9.06)	171% of minimum wage in 2017 (\$12.20)
Job Retention	90% to be employed after 12 months	Nearly 100% employed after 12 months
Business Formation	20% rate of formation	23% rate of formation Over 350 businesses launched by over 1,500 released graduates, including at least 5 that generate over \$1MM in annual revenue
Recidivism	Less than 10% (3-year basis)	7.5% (3-year basis, avg. of last 5 cohorts)

TEXAS EXPANSION

PEP began service at the Hamilton Unit in 2004-5, then moved to the Cleveland Unit in late 2007, where it continues to operate both its Leadership Academy and Business Plan Competition. Based on its success, PEP received TDCJ approval to expand into the Sanders Estes Unit in mid-2014. In 2017, PEP successfully launched the Leadership Academy program at the Gib Lewis unit, and began its program for women at the Lockhart Unit in late 2017. All of these are steps toward our goal of serving at least 4,000 men and women by 2026, which will represent about 10% of the population released from prison annually. Our recent and anticipated service levels are summarized below:

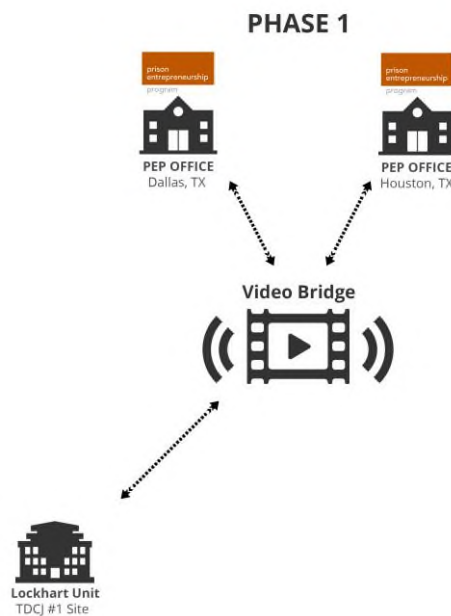
Men Served Inside					
UNIT	PROGRAM	2015	2016	2017	2018
Cleveland	Leadership Academy (LA)	312	304	318	320
	Business Plan Competition	258	212	228	237
Estes	Leadership Academy (LA)	171	244	288	300
	Business Plan Competition	57	140	179	215
Gib Lewis	Leadership Academy (LA)			41	133
Unit #4	Leadership Academy (LA)				90
	Business Plan Competition				
Total Men Served Inside		621	718	943	1,232
Women Served Inside					
UNIT	PROGRAM	2015	2016	2017	2018
Lockhart	Leadership Academy (LA)				90
	Business Plan Competition			44	32
Total Women Served Inside				44	130

Men Served Outside				
	2015	2016	2017	2018
Total Men Served Outside (Unduplicated)	214	238	297	387
Women Served Outside				
	2015	2016	2017	2018
Total Women Served Outside (Unduplicated)				23

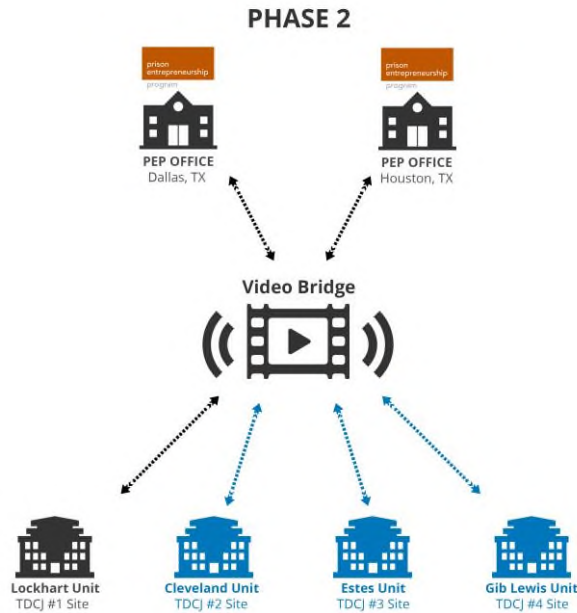
THE ROLE AND IMPACT OF VIDEO CONFERENCING

The CenturyLink Team proposes to equip a number of TDCJ units served by PEP (as well as PEP’s two main offices) with video conference (“VC”) capability to accelerate program expansion throughout Texas. This acceleration will result from incorporating proven “distance learning” techniques to reduce the travel time and costs of current staff and volunteers, and will enable the more efficient use of new staff and volunteers. At the same time, this should facilitate broader involvement by Executive Volunteers and other community members, further expanding the already strong PEP network that is so important in successful re-entry.

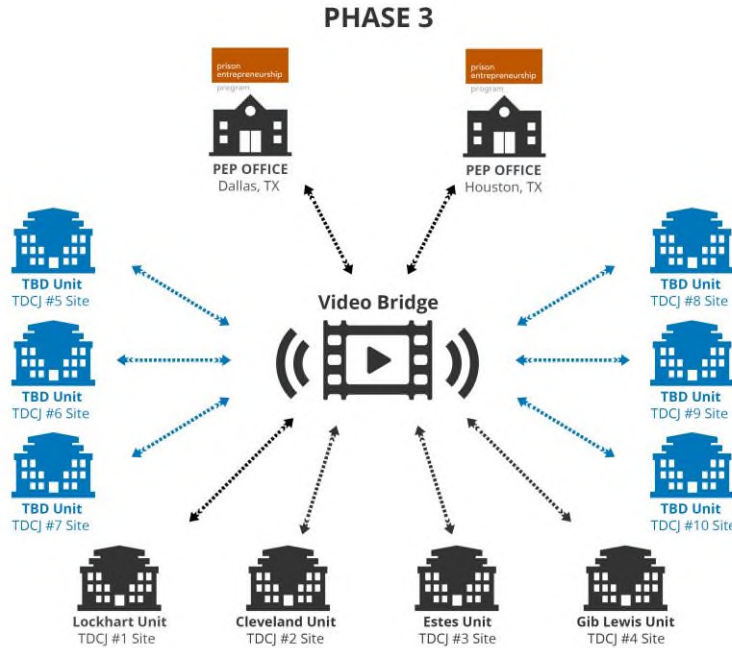
Phase 1 of the Project will include the addition of VC capability to PEP’s offices in Houston and Dallas, as well as to the Lockhart Unit where PEP currently runs its Leadership Academy and Business Plan Competition for women, connecting them via a secure, high-quality video “bridge.” This will allow staff and volunteer teachers / facilitators, whether based in Houston or Dallas, to lead classes at Lockhart without incurring the time and expense of a 4.5 hour (Houston) or 7 hour (Dallas) round trip drive.



Phase 2 of the Project will extend the benefits of these improved efficiencies and quality enhancements to the Cleveland, Estes and Gib Lewis units where PEP also currently operates. Furthermore, the unreleased PEP graduates (Servant Leaders) housed at Cleveland, for example, will be able to facilitate classes and effectively serve as mentors for men just entering the program at Estes and Gib Lewis (for example) in much the same way that they currently do for the men at Cleveland (and vice versa for the Servant Leaders at Estes in relation to the newly accepted men at the other units). Note, however, that we propose to limit these inter-unit connections to same sex classes. Further, all participation by Servant Leaders in VC connections with other units would of course be subject to security screening by TDCJ.



Phase 3 of the Project will extend the benefits of the proposed VC system to up to additional six TDCJ units, to be selected by mutual agreement of TDCJ, CenturyLink / Securus and PEP. Many TDCJ units are located more than an hour’s drive from any major metro area (where high quality Executive Volunteers, so critical to success, are more likely located). In addition, there are many men and some women in TDCJ who would benefit from PEP, especially the Leadership Academy, but have sentences that are so long they are unlikely to be eligible (within 3 years of release) before they are released on parole. Adding VC capability to additional units, including more remote units, would enable PEP not only to leverage its strong network of Executive Volunteers but to reach inmates who would otherwise never benefit from any part of PEP’s program.



OTHER BENEFITS

Once the VC infrastructure described in this proposal is built, significant additional benefits could be realized. For example, TDCJ could “piggyback” portions of the current peer health education curriculum delivery on the same platform. In addition, overcoming geographic and logistical restraints would enable PEP to recruit speakers, teachers and Executive Volunteers from any place in the country where a high quality VC connection is available. Not only might this significantly enhance the impact of PEP on the men and women it serves in Texas, but it could enhance the image of Texas as a leader in the smart use of technology to further reduce repeat and intergenerational crime.

Option #7 Cost = Add \$0.005 to base rate per minute to enable PEP VC at 10 total facilities

Added Value – Option #8 - Visitation Phone Monitoring (VPM)

Visitation Phone Monitoring (VPM) deployment includes enhancing security and investigative capabilities for onsite visitation. The enhancement introduces the deployment of SCP call monitoring and recording of non-contact visitations where visitors are only allowed to use a telephone handset to communicate with an offender using another handset while looking at each other through a glass or plexiglass partition. Installation includes new wiring to connect the visitation stations to the SCP platform.

The CenturyLink Team will work with the Department to identify facilities that would benefit from the VPM feature.

Option #8 Cost = Add \$0.002 to base rate per minute to enable 100 visitation sets (200 phones)

Added Value - Option #9 - Carrier Database Access

As a division of a Local Exchange Carrier (LEC), CenturyLink has unique access to carriers and reverse lookup databases, and continues to offer assistance whenever needed to State investigative staff. These unique relationships are augmented by our “closed loop” account setup process, which verifies Billing Name and Address information for all called parties upon account setup, and can make this information available to TDCJ.



Any investigator knows that even the most sophisticated investigative tools can be rendered useless if they cannot track the phone on the other end of the conversation. As a result of access to these databases, investigators receive verified billing name and address information for use in investigations.

Finally, even if a number outside the Offender Telephone System becomes part of an investigation, CenturyLink’s corporate law enforcement department and unique carrier relationships are available to our customers.

❖ CASE STUDY ❖

CenturyLink’s carrier relationships were put to the test in a murder cold case. After months of attempts by detectives to get a SIM card unlocked, CenturyLink management was able to use executive level contacts to unlock the SIM card in less than one week.

This was put to the test in a murder cold case at one of our County correctional customers – detectives there were unable to contact the right people to get a SIM card unlocked. Through CenturyLink’s LERG database and executive-level contacts at the carrier, we were able to contact the right people and get the SIM card unlocked in less than one week.

The LERG database provides carrier information, as well as alternate contact information for subpoena requests, for numbers that may not be entered into the system but may materialize in the course of an investigation.

Enhanced carrier database (LIDB)

Phone Number: 2520000000 * Format: NPANXXXXXX
 Select BNA Provider: Compiled Data Source (33)

Phone Number	2520000000
BNA Host Provider	Compiled Data Source (33)
Reply Code	800 - (Verify) Listing found and information can be found in the addenda of the response
Name	MANXXXXXXXXXX
Address	4014 WHITEH...
Service Start Date	11-15-2011
Company Type	C
OCN	0470
OCN Name	CENTURYLINK
Wireless Indicator	N
Ported Indicator	N
LIDB ID	UT
Timestamp	Thu Apr 12 14:59:23 EDT 2012

Local Carrier Routing Guide (LERG)

Network Services - Client Systems - NDA - LERG (Info)

LERG Switch Information Lookup
 Local Exchange Routing Guide - Switch Information
 Enter any one of the following criteria to search for LERG info:

CLI code (use OTHER CASE)
 Enter partial CLI for wildcard search - enter FL to find all entries with FL anywhere in the CLI.

NPA / NXX /
 Enter 3 digit NPA and either 3 digit or partial NXX for wildcard search.
 Example: entering 800-XXX and 800-400 will return 202-040-2940-940, 202-401, 202-402, etc.

LATA code
 Enter LATA for a list of all associated CLTs.

OCN
 Enter the Operating Company Number for detailed OCN information.

Local Routing Number
 Enter LRN per first four digits to list associated CLTs.

LATA **OCN**
 Enter LATA To find all NPA/NXX's for a LATA. (Entering an OCN will narrow the search).

OCN Category
 Select a category for a list of OCNs.

Actual Switch CLI
 Enter actual_cli_id for a list of all associated CLTs.

Call Agent Code

Operating Company Information
 Click here for a [Printer-Friendly](#) version of this page.

OCN: 9533
Name: SOUTHWESTERN BELL
Abbr. Name: SOUTHWESTERN BELL
Category: EBDC **State:** TX **over_all_size:** 9533

Contact Information:
Name: ADI **Phone:** 921-1500000
Title:
Company: SOUTHWESTERN BELL
Address: 26
SA:
Mainstep info: 159005

Operating Carrier Number and Name

Wireless vs. Wireline Indicator

Porting indicator - e.g. wireline to wireless

Through Enhanced LIDB and CenturyLink's exclusive access to LERG, additional Billing Name and Address information - in addition to carrier contact information for records requests - are available to authorized investigative personnel

Option #9 Cost = Included in base rate per minute

Added Value - Option #10 - THREADS Enhancement

THREADS is an exclusive investigative technology that no other provider can offer to the correctional industry. We are the only provider with the ability to offer seamless JPAY Financial data integration with THREADS, which is in use at TDCJ today. Other financial information from other sources can be imported into our THREADS tool as well. THREADS is available to the Department empowering the Department with the latest in investigative technology and one of the most powerful tools in the intelligence community.

Option #10 Cost = Included in base rate per minute

Added Value - Option #11 - Wireless Containment Service Denial

With the recent success of the Wireless Containment System (WCS) deployment at TDCJ, The CenturyLink Team is expanding our efforts to identify and eliminate the threat associated with contraband cellphone use within TDCJ facilities. As new technology and capabilities emerge, we are continually evaluating their viability and potential usage within the Department.

An emerging capability that is being vetted by industry officials and the Cellular Telecommunications Industry Association (CTIA) provides a way to shut down cellphones identified as contraband within a correctional facility without interfering with legitimate cellphone users nearby.

Once a cellphone is identified as contraband, using new or existing WCS techniques, that cellphone's information is prepared and sent to local authorities to obtain a court order that authorizes the carrier to shut off that cellphone's service. The court order process and the authorization to shut off the cellphone service is part of the checks and balances necessary to compel carriers to act on behalf of law enforcement agencies while providing meaningful assurance that the targeted cellphone is, in fact, contraband.

The CenturyLink Team has developed our capability around this industry initiative and has incorporated software techniques to identify these contraband cellphones. Once identified, they will be added to a service termination request and submitted through the court order solicitation process. All forms and filings have been streamlined with information required to justify the request for a court order and to simplify the judicial process.

The CenturyLink Team is pleased to offer this as a value added service to TDCJ and is eager to discuss it with you upon contract award.

Option #11 Cost = Included in base rate per minute

Added Value – Option #12 - Jobview Re-entry Software

The CenturyLink Team is proud to offer the Jobview 2nd Chance software for the Parole Division at TDCJ. The Jobview 2nd Chance product allows offenders returning to the community to search for statewide and nationwide jobs without direct access to the internet.



Jobview 2nd Chance provides access to nearly 2 million job listings. The listings are updated every 48 hours so users are always searching current jobs. A software only version of the Jobview 2nd Chance program is being offered with the assumption that the facilities already have a secure computing environment that is accessible by offenders.

Offender Benefits

- Get a 30-90 day head start on a job search
- Browse state and nationwide jobs that are current and updated every 48 hours
- Start thinking about jobs before release; putting their mind on something positive and productive
- See what skills and specific requirements they will face well ahead of release
- Match educational programs they are using to the types of jobs they may be qualified for and will likely encounter
- Practice electronic job searching which is technology they will commonly see upon release

Correctional Facility Benefits

- No job-seeker training costs because the Jobview 2nd Chance user interface is self-explanatory
- Staff no longer needs to find and print job listings for their transitioning offenders
- Job listings for all types of jobs and levels of experience in cities nationwide
- Previous cost for Jobview (grant funded) was approximately \$380,000 annually

Option #12 Cost = Included in base rate per minute for software only offer

Costs for deployment of kiosks can be negotiated if needed.

Added Value – Option 13 - High-Speed Satellite Network Services

As the Department is aware, many TDCJ sites are located in areas with poor quality and/or very high cost network connectivity. This situation impacts the CenturyLink Team in addition to the Units. We therefore offer TDCJ an opportunity to simultaneously test high-speed satellite services in parallel with CenturyLink. While wireline connectivity to the OTS will be maintained throughout the test period, CenturyLink would also be testing the new satellite network for consistent service quality for potential future service offerings.



Because our testing will not require all the bandwidth available through the satellite service, we offer 15 to 20 Mbps to TDCJ's use at two Units of its choice for up to 24 months.

Option #13 Cost = Included in base rate per minute for 2 year trial

Added Value – Option #14 – Mobile Contraband Cellular Assessment Program

Cellular Assessment is another tool in the fight against proliferation of Cell phone contraband within corrections. An assessment will assist the Department in determining the severity of the contraband cell phone problem by providing cellular access points at a correctional facility capable of identifying the number of cellular phones that attempt to communicate with local cellular carrier networks.

The Cell Phone Assessment solution works by deploying active cellular access points and targeting areas of the facility with mobile equipment that is capable of collection of contraband cell phone devices within the facility although the equipment is operated from outside the facility. Contraband cell phones within RF range of these active access points are registering cell phones using the cell phone's International Mobile Subscriber Identity (IMSI).

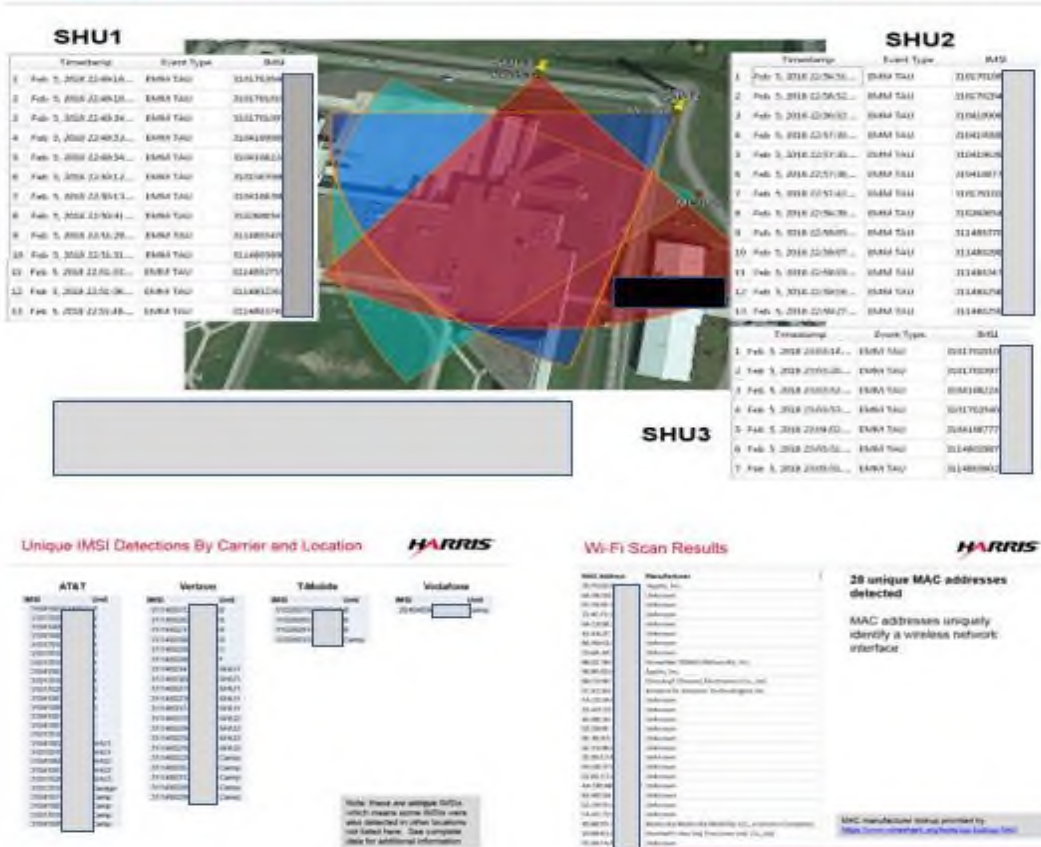
This solution is provided as a service; it is mobile and can be deployed to multiple sites. The Mobile Contraband Cellular Assessment is designed to detect and identify the presence of contraband cellular and Wi-Fi devices within a specified, controlled facility. The use of state-of-the-art, frequency and band -agile Software Defined Radios (SDR) to adjust to each unique RF environment is deployed with expert operators who carry out the assessment so the service is full turn-key for the Agency. The access points operate in the predominant 3G/4G/LTE bands and frequencies, for all carriers. Most devices, including all CDMA devices, are uniquely identified on the LTE protocol as a priority to the 3G and 4G technologies, whenever possible, providing the latest in technology advancements for this type application.

If contraband devices are detected, the unique identifiers of the device are captured for analysis and reporting to the agency. An average site can be assessed in one working day; the completed analysis and report are available approximately one week later.

After the facility is assessed, a report is generated and provided to the Department. The report contains the following information:

- Overview of the macro cellular networks in the area
- Date, time, location and coverage of each measurement
- Total number of International Mobile Subscriber Mobile Identity (IMSI) detections

- List of unique IMSI detections
- Mobile Carrier of each device
- Distribution of carrier usage
- Make and model of devices may be determined
- Approximate locations of devices
- Unique Wi-Fi MAC detections with approximate locations



Examples of data provided in the Assessment Report

Further investigative services are available in addition to this assessment, if desired by the Department, through our Investigative Services, including Forensics extraction and analyst services.

The final report will consist of the IMSI or account information of the contraband device. The CenturyLink Team offers an optional service to also assist with serving court order for historical, past 30 days use of those phones and process the information through our Investigative Services group using patented methods for high probabilities of identifying the offender or offenders' use of this device, or pattern of usages, for more successful shakedowns.

Information can also be provided with proper legal methods which The CenturyLink Team can assist in for call termination orders, if applicable.

Option #14 Cost = Add \$0.003 to base rate per minute to enable 60 mobile assessments

Added Value – Option #15 – Stationary Contraband Cellular Assessment Program

The Stationary Contraband Cellular Assessment Program is also a service to assist the Department in identifying contraband cell phones within correctional facilities.

CenturyLink also provides a stationary assessment system that includes deployment of a limited amount of fixed radios and base station at a facility to capture, identify and report on contraband cell phones during an extended assessment period – typically permanently installed until a decision is made to deploy a fully functioning managed access system.

This assessment will assist the Department in determining the severity of the contraband cell phone problem by identifying the number of contraband cellular phones that attempt to communicate with local cellular carrier networks.

The Stationary Deployment Program also includes the use of Guarded Exchange to conduct analysis of the contraband cell phone data collected.

Analytics may include cross-correlation of identifiers to assist with identifying probable inmate usage of devices based on information collected by the assessment system. Guarded Exchange may also prepare formal reports and documentation to support the Department with termination-of-service requests. These reports can be generated to provide the cellular telephone identities with the associated supporting documentation and carrier information needed to initiate a court-order process for a termination-of-service request.

Option #15 Cost = Add \$0.005 to base rate per minute for each stationary contraband assessment deployment.

Added Value – Option #16 - Guarded Exchange – Expanded

The CenturyLink Team is proposing the Guarded Exchange (GEX) Investigative Support Service (ISS) to assist the Department with 1) additional investigative abilities and 2) the Crime Tip program.

Additional Investigative Assistance

Upon contract award, the CenturyLink Team will increase the number of monthly calls monitored from 15,000 to 30,000 with incremental monitoring staff. In addition, we will hire two (2) full time employees to assist the Department under the direction of CID. With TDCJ approval, the CenturyLink Team will staff these positions using our internal human resources organization. All new hires will be subject to review and approval of the TDCJ and full background checks will be performed.

They will enhance TDCJ's investigative abilities by providing:

- Detailed training and support services for the CID. They will educate investigators in the use of THREADS, how to import data from various sources and how to run reports on the information obtained. Additionally, they will assist TDCJ in importing and analyzing data into THREADS to identify patterns of suspicious activity of offenders and outside parties from previously unrelated activities.
- Assistance to the Department to create customizable Organizations to aid in tracking investigations and building security threat group (STG) rosters. These customizable Organizations can be kept private or shared, within the Department, creating tremendous value for investigators.
- The manpower to incorporate and analyze WCS data. WCS Intelligence is processed through a series of cross correlation techniques utilizing Securus platforms which include but are not limited to SCP, IPRO, JPay and THREADS. The intelligence is further processed through GEX proprietary software and internal databases. This leads to identifiers of the user of the contraband cell phone or generates leads which point to the persons utilizing the device with a high degree of probability.

Crime Tip Assistance

Upon contract award, The CenturyLink Team will hire one (1) full time employee to assist in listening to and reporting on Crime Tip hotline calls. The CenturyLink Team will staff this position using our internal human resources organization. All new hires will be subject to review and approval of the TDCJ and full background checks will be performed.

The Crime Tip program administers an offender crime reporting tool that provides an anonymous and secure way for offenders to communicate crime tips to the TDCJ investigative staff. The CenturyLink Team's Secure Call Platform (SCP) anonymously records and stores all messages left on the Crime Tip Hotline, so an offender doesn't have the risk of being identified as an informant.

Offenders may 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 by default, informants may choose to leave their name.

The CenturyLink Team Crime Tip program includes:

- A pre-arranged telephone number (designated by the facility), provided to all offenders
- 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 offender

Option #16 Cost = Included in base rate per minute

Added Value – Option #17 - Televisit

The CenturyLink Team partners with PHD Medical (a Securus Company) to offer the Televisit™ telemedicine solution. Agencies can reduce the number of external offender transports, reduce staffing costs, and increase public safety through telemedicine. Any medical practitioner at any location with a computer and Internet connection can conduct routine evaluations, specialty consultations, and emergency medical examinations without the need to transport inmates. Televisit is a **FDA-approved** telemedicine suite specifically built to integrate with a host of medical devices required for medical examinations. The remote practitioner controls the high-resolution camera and diagnostic devices requiring little training for facility staff.

Facilities can use Televisit for:

- Scheduled health clinics for hypertension and diabetes management
- Perform psychological evaluations and clinical sessions for other mental health issues
- Exams with specialists such as Dermatology, Neurology, Cardiology
- Emergency examinations to determine need to transport a patient to an outside facility

The CenturyLink Team and the Department can negotiate a full deployment of this service upon contract award. An initial deployment of Televisit includes the following:

- Four (4) fully loaded telemedicine carts
- Subscription fee to service 10,000 offenders
- 400 Technical Consultations per month



Option #17 Cost = Add \$0.004 to base rate per minute

Added Value – Option #18 - Tetrus PREA Trac

The CenturyLink Team is proud to offer the Tetrus PREA Trac software. The PREA Trac application is a software case management tool that allows correctional facilities to document, monitor, and report on investigations conducted based on sexual allegations. PREA Trac assists these correctional facilities by documenting cases of assault while providing them with reporting guidelines that minimize risk and ensure compliance with Federal and State PREA laws.



Value:

- Operationalizes PREA compliance
- Automates PREA reporting with processing, collecting, analyzing, and reporting capabilities
- Mitigates Risk - Class Action Awards: Michigan paid \$100M, Washington, D.C. paid \$50M

Benefits:

- Ensures PREA Reporting compliance
- Supports and enhances audit procedures relating to PREA
- Provides a repeatable and compliant best practices process
- Provides alerts and call to action when items fall outside of compliance
- Automates the documentation and reporting submittal of PREA incidents to BJS
- Provides dashboard visibility of trends and patterns helping to create, maintain and improve safety
- Supplements reduced staff via Full Time Equivalent (FTE) efficiency gains

Features

The Tetrus PREA *Trac* software product enables you to report, track, and comply with the reporting guidelines of the PREA law. PREA *Trac* includes the following features:

- Tracks the PREA compliance after the sexual allegation filing.
- Documents all actions required for compliance with the PREA law.
- Automatically generates the required federal reports to be sent to the US Department of Justice.
- Easy to deploy since PREA *Trac* is a secured cloud-based application that can be deployed readily. This can also be deployed as an on premise application, if required by the facility
- Operates independent of any Offender Management System (OMS) application, but is architected for easy integration if needed.
- Easily configurable to meet the unique needs of large facilities such as State Departments of Corrections
- Accommodates workflows, multiple facilities, & additional data points.
- Can be set up as a central database as well as an individual database for large statewide agencies with multiple sites. Users, based on the role assigned, will be able to access individual sites or all the sites system wide. The data can be organized by facility or aggregated.
- Information is partitioned by agency and access to data is controlled by agency and roles. A confidentiality agreement for users to read and sign when they first log into the system will be provided.
- Users are vetted and authorized by the local agency. Only these authorized users can access PREA *Trac* on the Secure Cloud or using an on premise model. This provides investigative data security.
- Investigators or the PREA Manager can initiate investigations, however only the PREA Manager can authorize the final outcome.

- Unlimited Training is provided by Tetrus throughout the duration of the contract.
- Support for report changes as required by the US DOJ included in the cost of the product.
- In addition to the prebuilt reports and dashboards provided, Tetrus can make additions or modifications or the State can also build your own custom reports and dashboards.

PREA *Trac* has been designed and developed based on best practices obtained from the Massachusetts Department of Correction, which is a pioneer in developing an automated way of managing PREA cases. In addition, this product has also been refined based on input from Dr. Reginald Wilkinson, ex-Director of the Ohio Department of Corrections who has been intimately involved in the development of the PREA law and is a Chair of the Prison Rape Committee as well as Richard Roy who is an ex-Deputy Commissioner for the New York State Department of Correction. In addition, the some other State DOCs such as the New York State Department of Correction has reviewed the product and liked the functionality reflected in this product. PREA *Trac* is currently installed in 35 correctional facilities across 17 states.

Option #18 Cost = Add \$0.003 to base rate per minute

Added Value – Option #19 - Wireless Containment Services - Additional Facility

The CenturyLink Team is proposing an optional third Wireless Containment Solution (WCS) to build on the successes at McConnell and Stiles. The proposed WCS is the combination of a managed private cellular telephone network and a tightly controlled RF Distributed Antenna System (DAS) similar to the what has already been installed at TDCJ.



The WCS allows the Department to effectively manage contraband cellphones by containment, while allowing communications to legitimate wireless communications within the designated areas of the prison and without impacting cellphones outside the TDCJ Unit in public areas.

The Wireless Containment Solution offers:

- The installation of a system which combines a specially managed cellular telephone network and precisely controlled RF through a Distributed Antenna System (DAS).
- A WCS solution capable of managing all 2G, 3G, and 4G technologies, protocols and frequency bands used by Wireless cell phone carriers within the United States.
- The ability to manage mobile devices and apply policy rules, as determined by the Department’s administrators, to either allow or disallow cellular telephone communications.
- A fully automated solution which manages all cellular telephone access 24/7-365 days a year. Including prevention of inmates’ attempts to post to social media.
- Complete administrative control capabilities both locally and remotely. Allowing the CenturyLink Team to offer the Department a complete management and maintenance of the WCS with minimal TDCJ resources needed for escorts during periodic site visits.

- 24/7/365 active monitoring and support through the CenturyLink Team's Network Operations Center. The WCS managed solution requires little or no special training, additional staff or significant commitment of time by TDCJ personnel

The addition of an optional third WCS at another TDCJ Unit will to continue to expand the Department's ability to control the unauthorized use of contraband cellphones. As evidenced by our previous TDCJ successes, the CenturyLink Team's WCS is the most effective weapon against contraband cellphone usage in the industry today.

The CenturyLink Team is pleased to offer this as a value added service to TDCJ and is eager to discuss it with you upon contract award.

Option #19 Cost = Add \$0.012 to base rate per minute

VOLUME TWO, SECTION
2 – SOLICITATION
COMPLIANCE AND
EXCEPTIONS

Volume Two , Section 2 - Solicitation Compliance and Exceptions

- A. In this Section, the Proposer shall respond to each requirement of Sections D through I, inclusive of the RFP and indicate whether it proposes to comply.**
- B. For the purpose of facilitating discussions, for every instance where the Proposer does not propose to comply or agree to a requirement, the Proposer shall propose an alternative and describe its reasoning therefore.**
- C. It is not necessary to respond on a paragraph by paragraph basis except as required for clarity; for example, if the Proposer agrees to the terms of Sections E through I of the RFP in its entirety, a single statement to that effect will suffice.**

CENTURYLINK HAS READ, UNDERSTANDS AND COMPLIES

Beginning on the following page, please find our response to Sections D-I.

SECTION D - REQUIRED REPORTS

D.1 REPORTS REQUIRED FROM CONTRACTOR

A variety and number of reports are required to be submitted by the Contractor during the course of the Contract. These reports may be revised or additional reports may be required at the Department's sole discretion.

Contractor is required to provide standard, ad hoc, and special request reports. Standard reports (ref. Exhibit J.9) will be used by the Department to monitor day-to-day performance. Contract progress will be monitored through review and analysis of status and management reports submitted to the Department's Contract Monitor. Contractor may be required to submit examples of standard reports which are accessible directly from the system database(s).

The Department reserves the right to request optional or additional reports that may be considered "ad hoc" reports or special request reports not specifically identified in this Contract. These reports shall be delivered no later than three (3) business days from the date of request unless special circumstances exist. If special circumstances exist, e.g. the report would require special research and /or IT development, Contractor will work with the Department to provide the report in a reasonable and mutually agreed-upon timeframe.

The Department may also request revision of existing reports as deemed necessary throughout the term of this Contract. The Contractor shall adapt report/documentation formats and delivery to meet Department requirements.

Contractor shall provide electronic and/or hard copy reports no later than an agreed upon date (e.g. viewable format on-line or as batch print reports). Due to the large number of reports required by the Department, reports shall be made available to authorized Department staff and may be required to be sent to or accessed from several locations throughout the State. Due dates and Department staff receiving reports will vary dependent upon the type of report. Report titles and other field identifiers may be customizable by the authorized Department staff.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION D.

SECTION E - INSPECTION AND ACCEPTANCE

E.1 INSPECTION OF SERVICES

- A. The Department and other Government regulatory agencies have the right to inspect and test all Services called for by this Contract, to the extent practicable at all times and places during the Contract Term. The Department shall perform inspections in a manner that will not unduly interfere with the Contractor's operation and management of the program. The Contractor shall furnish, and shall require subcontractors to furnish, at no increase in the Contract price, all reasonable assistance for the safe and convenient performance of these duties.
- B. From time to time the Department shall, subject to limitations provided by law with respect to rights of privacy, have the right to reasonably prompt access and to examine all records of the Contractor related specifically to the program, including financial records, employee records (including time and attendance records), and Offender records generated by the Contractor and its subcontractors in connection with the performance of this Contract.
- C. If subject to the outcome of an audit or inspection, it is determined that the Contractor is in non-compliance with any provisions of this Contract, and/or that money is owed to the Department by the Contractor, then the Department may exercise its rights of recovery of money owed as authorized.
1. If any of the Services are non-compliant with the Contract requirements, as identified by the Department; the Contractor shall be notified describing the specific areas of non-compliance. The Contractor shall have a twenty (20) Day period to file a written response detailing corrective action(s) taken to all items of non-compliance. The response shall include supporting documentation which verifies execution of corrective action(s) taken. Unless otherwise specified, or previously agreed to by the Department, the submission of a corrective action plan shall not be accepted as corrective action. For all items of non-compliance satisfactorily resolved by agreement between the Contractor and the Department, no further action regarding such items shall be taken. Any areas of non-compliance shall be corrected within twenty (20) Days or by the date of the Department approved extension.
 2. If any of the Services are non-compliant with the Contract requirements, as identified by a Government regulatory agency, the Contractor shall resolve all items identified as non-compliant by the deadline established by the agency.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION E.1.

E.2 INSPECTION OF PROGRAM

- A. The Contractor shall provide and maintain an inspection system acceptable to the Department covering the programs and work called for by this Contract. Complete records of all inspection work performed by the Contractor shall be maintained and made available to the Department during Contract performance and for as long afterwards as the Contract requires.**
- B. The Contractor shall provide entry at all times by the Texas Board of Criminal Justice (TBCJ) and the Department's authorized employees/agents for inspections and other official purposes. The Governor, members of the Legislature and all other members of the Executive and Judicial Departments of the State, as well as any other Persons designated by the Department, including the Office of the Inspector General, shall be allowed to monitor the delivery of Services.**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION E.2.

E.3 MONITORING CRITERIA

- A. The Department shall devise its own procedures for monitoring the quality of the Contractor's performance under this Contract, all Court Orders and Department Policies.**
- B. The Contractor shall cooperate fully with the Department in obtaining the requisite information needed to complete such audits and to assess the quality of the Contractor's performance.**
- C. Monitoring may include, but is not limited to, document reviews and on-site audits conducted by Authorized Representatives of the Department. Such monitoring by the Department shall not relieve the Contractor of any of its obligations under this Contract.**
- D. The Contract Monitor and other Department staff shall provide written findings regarding non-compliant conditions, processes, procedures or operations implemented at the facility, and observations that could, if not addressed by the Contractor, become an item of non-compliance as described in Section E.1.**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION E.3.

E.4 AUTHORITY TO AUDIT

- A. The Contractor understands that acceptance of funds under this Contract acts as acceptance of the authority of the State Auditor's Office (SAO), or any**

successor agency, to conduct an audit or investigation in connection with those funds. The Contractor further agrees to cooperate fully with the SAO, or its successor, in the conduct of the audit or investigation, including providing all records requested.

- B. The Contractor shall ensure that this Clause concerning the authority to audit funds received indirectly by subcontractors through the Contractor and the requirement to cooperate is included in any subcontract it awards.
- C. The Contractor shall reimburse the State of Texas for all costs associated with enforcing this provision.
- D. See Section H.8, Books and Records, concerning record retention.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION E.4.

E.5 AUDITS BY OTHER AGENCIES

Upon receipt of audits or monitoring reports pertaining to the provision of Services under this Contract that are conducted by agencies or entities other than the Department, the Contractor shall provide copies thereof to the Department within thirty (30) Days. The Contractor shall provide to the Department copies of responses to audits and/or inspections within seven (7) Days of issuance. Audits or inspections may include allegations or complaints involving program operations or the Contractor and its employees (including consultants, independent contractors and their employees, agents, and volunteer workers).

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION E.5.

E.6 FRAUD, WASTE OR ABUSE

- A. In accordance with Texas Government Code, Chapter 321, the SAO is authorized to investigate specific acts or allegations of impropriety, malfeasance or nonfeasance, in the obligation, expenditure, receipt or use of State funds.
- B. If there is a reasonable cause to believe that fraud, waste or abuse has occurred at this agency, it can be reported to the SAO by calling 1-800-892-8348 or at the SAO's website at www.sao.texas.gov. It can also be reported to the TDCJ Office of the Inspector General at 1-866-372-8329, the TDCJ Internal Audit Division at 936-437-7100, or Crime Stoppers at 1- 800-832-8477.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION E.6.

SECTION F - DELIVERIES OR PERFORMANCE

F.1 PERIOD AND PLACE OF PERFORMANCE

The term of the Contract will be from September 1, 2018 through August 31, 2025. The Contractor shall be required to perform services at the Department locations identified in the Site List (Exhibit J.1), under the general supervision of assignment by the Department's authorized staff. The Department may add, delete, or change site locations, and alter configurations of current Offender populations at any site location at any time. Where any work under this Contract requires access to secured facilities by the contractor's employees/subcontractors, it shall be the responsibility of the Contractor to comply with all pertinent security requirements, which shall be supplied by the Department. It is the sole responsibility of the Department to guarantee necessary site access.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION F.1.

F.2 OPTION TO RENEW

The Department reserves the right to renew this Contract for three (3) - two (2) year option periods. The Department will notify the Contractor as per Section 1.15.

The Contract will consist of a Base Period:
Seven (7) years (September 1, 2018 through August 31, 2025)

and three (3) two (2) year renewal Option Periods:

September 1, 2025 through August 31, 2027
September 1, 2027 through August 31, 2029
September 1, 2029 through August 31, 2031

All work shall be completed within the Contract period, unless otherwise extended by written modification of the Contract upon agreement of the contracting parties.

Contractor shall not begin performance until receipt of a written Notice to Proceed.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION F.2.

F.3 OPTION TO EXTEND

The Department may require continued performance of any Services within the limits and at the rates specified in this Contract. The Department reserves the right to extend this Contract for a ninety (90) Day period at the end of each Contract and/or renewal period for the purpose of re- advertising the Service, awarding a new Contract, and transitioning into a new Contract. The option to extend provision may be exercised more than once, but the total extension of performance hereunder shall

not exceed six (6) months. The Department may exercise the option by written notice to the Contractor within the period specified in Section 1.16.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION F.3.

F.4 TRANSITION OF CONTRACT

In the event services end by either Contract expiration or termination, it shall be incumbent upon the Contractor to continue services, if requested by the Executive Director or designee, of the Department, until new services can be completely implemented and operational. The Contractor acknowledges its responsibility to cooperate fully with the replacement Contractor and the State to ensure a smooth and timely transition. Such transitional period shall not extend more than one hundred eighty (180) days beyond the expiration date of the Contract, or any extension thereof.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION F.4.

SECTION G - CONTRACT ADMINISTRATION DATA

G.1 CLAUSES INCORPORATED BY REFERENCE

This Contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contract Specialist will make their full text available.

Texas Government Code, Chapter 2251, Payment for Goods and Services
CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION G.1.

G.2 AUTHORITY - AUTHORIZED REPRESENTATIVE, CONTRACT SPECIALIST, CONTRACT MONITOR AND PROGRAM DIRECTOR

G.2.1 Authorized Representative

- A. In the case of the Contractor, its President or any Vice President, shall designate the Authorized Representative in writing. The designation of the Contractor's initial Authorized Representative shall be delivered to the Department no later than the effective date of this Contract. The Contractor's Authorized Representative may designate other Persons to assist such Authorized Representative in the performance of certain obligations required by this Contract.
- B. In the case of the Department, the Executive Director is hereby designated as its Authorized Representative. The TDCJ Chief Information Officer has been designated as the Authorized Representative to act on behalf of the Executive Director on all matters pertaining to the daily operations and management of the program and in compliance with this Contract. The Department's Authorized Representatives may designate other Persons to assist such Authorized Representatives in the performance of certain obligations of this Contract.
- C. At any time, any party may designate any Person as its Authorized Representative by delivering to the other party a written designation signed, if on behalf of the Contractor, by its President or any Vice President, or if on behalf of the Department, by the Executive Director. Such designations shall remain effective until new written instruments are filed with or such notice is given to the other party that such designations have been revoked.
- D. The Department's Authorized Representative (the Executive Director) is the only Person authorized to make or approve changes in any of the requirements of this Contract, and notwithstanding any Clauses contained elsewhere in this Contract, the said authority remains solely with the Executive Director. In the event the Contractor makes any change at the direction of any Person other

than the Executive Director, the change will be considered to have been made without authority and no adjustment will be made in the Contract price to cover any increase in cost incurred as a result thereof.

G.2.2 Contract Specialist

- A. The Contract Specialist for administration of this Contract is Terri Bennett, CTPM, CTCM.**
- B. The telephone number for the Contract Specialist is (936) 437-7158.**
- C. The facsimile number for the Contract Specialist is (325) 223-0310.**
- D. The e-mail address for the Contract Specialist is terri.bennett@tdcj .texas.gov.**
- E. The Contract Specialist is responsible for general administration of this Contract, negotiation of any changes and final issuance of written changes/modifications to this Contract. All requests by the Contractor to modify the Contract shall be made in writing to the TDCJ Executive Director, and a copy submitted to the Contract Specialist.**

G.2.3 Contract Monitor

- A. The Contract Monitor is not authorized to make any representations or commitments of any kind on behalf of the Executive Director of the Department or the State of Texas.**
- B. The Contract Monitor does not have the authority to alter the Contractor's obligations or to change the Contract specifications, prices, terms or conditions.**
- C. If, as a result of technical discussions, it is desirable to modify Contract obligations or the statement of work, changes will be issued in writing and signed by the Executive Director of the Department.**

G.2.4 Program Director

The Contractor shall provide a Program Director for this Contract who shall be responsible for the overall management and coordination of this Contract and shall act as the central point of contact with the Department. The Program Director shall have full authority to act for the Contractor in the performance of the required Services. The Program Director, or a designated representative, shall meet with the Contract Monitor to discuss problems as they occur.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION G.2.

G.3 COMMISSION REMITTANCE

G.3.1 Remittance by Direct Deposit

It is recommended the Contractor remit payments via electronic funds transfer (EFT), also known as direct deposit to:

Texas Department of Criminal Justice Cashiers Office:
Att.: Stacie Tatom-Rodgers
PO Box 4015
Huntsville, TX 77342-4015

G.3.2 Late Remittance

Commission payment for any month is due by the **5th-business 20th** calendar day of the following month. Any amount owed to the State more than one (1) business day beyond the date such amount is due shall accrue interest each day at the rate of one percent (1%) plus the prime rate as published in the Wall Street Journal on the first day of July of the preceding fiscal year that does not fall on a Saturday or Sunday.

G.3.3. Commission Reporting

Commission report is due to the Department by the 20th day of the month following the month for which the revenue is due.

G.3.4. Review of Reported Revenue

The Contractor will review commission data with the Department each month to ensure previously reported revenue was accurate. In the event agreed commission payments for one (1) or more previous months are found to be in error, the associated payment adjustment will be made in the following month's revenue payment and without interest.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION G.3.

G.4 Annual Financial Disclosure Reports

- A. The Contractor shall have an annual audit performed by an independent Certified Public Accountant (CPA) and submit to the Contract Specialist the financial reports prepared according to Generally Accepted Accounting Principles and Auditing Standards (GAAP and GAAS) within one hundred twenty (120) Days after the end of the Contractor's fiscal year.
- B. In the disclosure of its financial affairs, the Contractor agrees to allow the Department or its representative's access to all its corporate books, to cooperate in any audits thereof and to provide the Department's Contract Specialist with 1 and 2 below:

1. **Consolidated financial statements such as are required by GAAP of the Contractor and its affiliates for such year, setting forth in each case in comparative form the corresponding figures for the preceding fiscal year, all in reasonable detail and certified by independent CPA's of recognized standing to the effect that said financial statements fairly present, except as specifically stated, the consolidated financial position and result of operations of the Contractor and its affiliates as of the end of the year for the year involved, and a statement signed by a senior accounting or financial officer of the Contractor that such officer has no knowledge, except as specifically stated, of the occurrence and continuance of any Event of Default or event which, with the time or the giving of notice, or both, would constitute an Event of Default (as defined in Section 1.3.1) or, if such circumstance does exist, specifying the nature and extent thereof and the actions proposed to cure same; and**
2. **Copies of any "management letters" (as that term is understood pursuant to GAAP and GAAS) received by the Contractor following any such audits.**

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION G.4.

SECTION H - SPECIAL CONTRACT REQUIREMENTS

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH SECTION H, WITH EXCEPTIONS NOTED.

CenturyLink has made certain modification redlines to the Insurance Requirements of the RFP in order to comply with our insurance carriers' policies. These redlines are shown clearly within the text, with comments on our reasoning where appropriate.

H.1 INSURANCE REQUIREMENTS

- A. Prior to the approval of this Contract by the Department, the Contractor shall procure, pay for and maintain the following insurance written by companies approved by the State of Texas and acceptable to the Department. It is recommended that coverage be with a company or companies having both, a Financial Strength Rating of "A" or better and Financial Size Category Class of "VII" or better from A.M. Best Company, Inc.
- B. The insurance shall be evidenced by delivery to the Department of certificates of insurance executed by the insurer or its authorized agent stating coverage, limits, expiration dates and compliance with all applicable required provisions.
- C. Upon request, the Department shall be entitled to **receive review** without expense, copies of the **redacted** policies and all endorsements. Copies and changes to the initial insurance **policies-certificates**, including extensions, renewals, cancellations and revisions shall be submitted to the Contract Specialist within thirty (30) Days of the effective date.

***CenturyLink Comment:** Policies are proprietary to both CenturyLink and our carrier, and unable to be released. CenturyLink does offer to provide redacted copies for the Department's review upon request.*

- D. Subject to the Contractor's right to maintain reasonable deductibles, the Contractor shall obtain and maintain in full force and effect for the duration of this Contract and any extension hereof, at the Contractor's sole expense, insurance coverage in the following type(s) and amounts:
 - 1. Workers' Compensation with statutory limits; Employers Liability with minimum limits for bodily injury:
 - a. By accident, \$1,000,000 per each accident; and
 - b. By disease, \$1,000,000 per employee with a per policy aggregate of \$1,000,000.

2. Commercial Automobile Liability Insurance covering owned, hired, and non-owned vehicles, with a minimum combined bodily injury (including death) and property damage limit of \$1,000,000 per occurrence.
3. Commercial General Liability Insurance including, but not limited to, Premises/Operations, Personal & Advertising Injury, Products/Completed Operations, Independent Contractors and Contractual Liability with minimum combined bodily injury (including death) and property damage limits of \$1,000,000 per occurrence, and \$2,000,000 general aggregate.
 - a. Civil Rights Liability shall be provided with the same liability limits. It may be included with the General Liability policy or written on a separate policy.
 - b. The Department shall be named as an additional insured by using endorsement CG2026 or broader.
4. Professional Liability (only if professional services are needed) including coverage for the rendering of, or failure to render, professional services with minimum limits of \$1,000,000 per occurrence, \$3,000,000 annual aggregate. Coverage to include errors and omissions.
5. Commercial Crime Insurance to cover losses from Employee Dishonesty with a minimum limit of \$1,000,000 each occurrence endorsed to cover third party property. The Department must be joint loss payee.

NOTE: If the insurance described in 3 or 4 above is written on claims-made form, coverage shall be continuous (by renewal or extended reporting period) for not less than sixty (60) months following completion of the Contract and acceptance by the Department. Coverage, including any renewals, shall have the same retroactive date as the original policy applicable to this Contract.

H.1.1 Required Provisions

The Contractor agrees that with respect to the above required insurance, all insurance contracts and certificate(s) of insurance will contain **and state, in writing**, the following required provisions:

- A. **Include Name** the Department and its officers, employees and elected representatives as additional insured to all applicable coverages.

***CenturyLink Comment.** Given CenturyLink, Inc.'s size and wide customer base, it is unable to modify policies to explicitly name each individual customer. However, it achieves this same objective through blanket additional insured endorsements for all customers.*

- B. Waive subrogation against the Department, its officers, employees, and elected representatives for bodily injury (including death), property damage or any other loss, to all applicable coverages **to the extent caused by CenturyLink.**
- C. Provide that the Contractor's insurance is the primary insurance in regards to the Department, its officers, employees and elected representatives.
- D. Provide that all provisions of this Contract concerning liability, duty and standard of care, together with the indemnification provision, shall be underwritten by contractual liability coverage sufficient to include such obligations within applicable policies **to the extent coverage is commercially standard.**
- E. Ensure that all certificates of insurance identify the Service or product being provided and the name of the responsible party.
- F. The Contractor, through an insurance agent licensed by the State of Texas, shall obtain all insurance coverage and an insurance company **authorized licensed** to issue such coverage in this State shall provide such coverage. No "self-insurance" coverage shall be acceptable. All policies shall include a provision requiring at least thirty (30) Days prior written notice of cancellation to the **Department Contractor with contractor providing a copy of such notice to the Department within ten (10) business days.**

***CenturyLink Comment.** Certain insurance coverages require only authorization not formal licensing. Regarding notification, our carriers cannot agree to notify individual customers; however, CenturyLink commits to prompt notification of TDCJ in the unlikely event of cancellation.*

- G. All insurance coverage obtained by the Contractor shall continue in full force and effect during the Contract Term. No contract shall be entered into between the Contractor and the Department unless insurance coverage binders are received by the date scheduled for the execution of the contract. Proof of insurance policies must be delivered prior to the Service Commencement Date.
- H. The Contractor may choose the amount of deductible for any other insurance coverage required (above) to be obtained by the Contractor, which shall be maintained at commercially reasonable levels. **but in no event shall such deductible for each occurrence exceed five percent (5%) of the required yearly aggregate limit of coverage.**

***CenturyLink Comment:** CenturyLink maintains aggregate insurance coverages appropriate for a company of its size and financial capability, and respectfully requests this redline.*

- I. The Contractor is responsible for the first (1st) dollar defense coverage. All general liability **and professional liability** policies shall provide defense in addition to the policy limits.

CenturyLink Comment: Defense costs are unfortunately not available for purchase on professional liability insurance.

- J. The limits required herein are minimum acceptable. However, these limits are not to be construed as being the maximum any prospective contractor may wish to purchase for their own benefit.
- K. As respect to the total limits of liability required, any combination of primary and/or umbrella coverage may satisfy those totals. However, if an umbrella is used, coverage must be at least as broad as the primary coverage.

H.2 SUBCONTRACTORS

- A. The Contractor may subcontract for the performance of any of its responsibilities to provide Services pursuant to this Contract.
- B. No subcontract may be entered into unless the Department provides prior written approval, which approval may not be unreasonably withheld.
- C. If a subcontractor is deemed to be needed for an event of an emergency nature, verbal approval may be obtained through an Authorized Department Representative. The Contractor shall submit a written request with supporting documentation for approval, by the Department, as soon as possible.
- D. The Contractor shall furnish to the Department copies of all subcontracts, without regard to the amount of annual payments.
- E. Any arrangement by the Contractor with an affiliate or member company to provide Services for the Program shall be subject to the subcontractor provisions of this Section.
- F. No contractual relationship shall exist between the Department and any subcontractor and the Department shall accept no responsibility whatsoever for the conduct, actions, or omissions of any subcontractor selected by the Contractor.
- G. The Contractor shall be responsible for the management of the subcontractors in the performance of their work.

- H. A subcontractor may not work directly with the Department in any manner and shall not be included in Contract negotiations, renewals, audits or any other discussions except at the request of the Department.
- I. Unless waived in writing by the Department, the subcontract shall contain the following:
 - 1. An acknowledgement that the subcontract is subject to the Contract between the Department and the Contractor (the "Master Contract").
 - 2. The subcontractor shall agree to comply with the terms of the Master Contract to the extent applicable with respect to goods and Services being provided under the subcontract. It is the intention of the parties of the subcontract that the subcontractor shall "stand in the shoes" of the Contractor with respect to fulfilling the duties and obligations of the Contractor to the Department under the Master Contract.
 - 3. The Department's approval of a subcontract does not relieve the Contractor of its duty to perform under the Master Contract.
 - 4. The Department shall be deemed a "third party beneficiary" to the subcontract.
 - 5. The subcontract shall contain the required Authority to Audit Clause referenced in Section E.4, and the required Non-Discrimination Clause referenced in Section 1. 12.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION H.2

H.2.1 Insurance

The Contractor shall require all subcontractors to obtain, maintain, and keep in force insurance coverage in accordance with accepted industry standards and the Contract during the time they are engaged hereunder.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION H.2.1.

H.2.2 Historically Underutilized Business (HUB)

- A. The Contractor shall make a good faith effort to award necessary subcontracts to HUBs in accordance with Texas Government Code, Sections 2161.181, 2161.252(b), and Texas Administrative Code, Title 34, Part 1, Chapter 20, Subchapter D, Division 1, Rule 20.285. Pursuant to the Statewide Procurement Division HUB Rules, Texas Administrative Code, Title 34, Part 1, Chapter 20, Subchapter D, Division 1, Rule 20.285, the Contractor shall submit a HUB

Subcontracting Plan (HSP) as part of the proposal submission, as well as make a good faith effort to implement the HSP. The Contractor shall seek written approval from the Department prior to making any modifications to its HSP.

- B. A detailed description of the HSP and required forms to be submitted with the proposal submission are included as Exhibit J.2.
- C. The Contractor shall provide notice to all subcontractors of their selection as a subcontractor for this Contract. The notice must specify, at a minimum, this Agency's name, the name of the Contract Specialist, this Contract's assigned Contract number, the subcontracting opportunity the subcontractor will perform, the approximate dollar value of the subcontract and the expected percentage of this Contract's total value that the subcontract represents. A copy of the notice shall be provided to the Contract Specialist no later than ten (10) working days after this Contract is awarded.
- D. The Contractor shall submit to the Contract Specialist on a monthly basis (by the fifth [5th] of the following month) the Prime Contractor Progress Assessment Report, which is included in Exhibit J.2.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION H.2.2.

H.3 TRANSITION

- A. Upon termination of this Contract, the Contractor agrees to work with the Department under the Department's management supervision for a period of sixty (60) Days, prior to the expiration of the Contract, to ensure the orderly transfer and efficient transition from current Contractor management to either the Department management or management by a third party of the program.
- B. During this transition period, the Contractor shall transfer all Offender records to the Department if requested to do so by the Department. In the event the Contractor requires copies of any records after Contract expiration and program management transition, the Department will furnish copies to the Contractor at the Contractor's expense.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION H.3.

H.4 RESERVED FOR FUTURE USE

H.5 UTILIZATION OF PRODUCTS AND MATERIALS PRODUCED IN TEXAS

- A. The Contractor shall comply with Texas Government Code, Section 2155.4441, relating to service contract use of products produced in the State of Texas.

- B. In performing Services under this Contract, the Contractor shall purchase products and materials produced in the State of Texas when they are available at a price and time comparable to products and materials produced outside of Texas.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION H.5.

H.6 CRIMINAL HISTORY INFORMATION COMPLIANCE

The parties hereto acknowledge and agree that in order for the Contractor to perform the Services contemplated herein, the Department may have to provide the Contractor with, or the Contractor may have access to, certain information regarding Offenders and former Offenders known as "criminal history information." Criminal history information means information collected about a Person by a criminal justice agency that consists of identifiable descriptions and notations of arrests, detentions, indictments, information and other formal criminal charges and their dispositions. The term does not include information as to convictions, fingerprint information, and driving records. In the event the Department provides the Contractor with criminal history information, the Contractor agrees to comply with the confidentiality requirements of 28 CFR 20.21; 42 U.S.C. 3711, et seq., as amended; and Texas Government Code, Section 411 .083; and with the FBI Criminal Justice Information Services (CJIS) Security Policy. More specifically, the Contractor agrees and acknowledges as follows:

- A. The Department hereby specifically authorizes that the Contractor may have access to criminal justice history to the extent such access is necessary or appropriate to enable the Contractor to perform the Services contemplated herein.
- B. The Contractor agrees to limit the use of such criminal justice information for the purposes set to herein.
- C. The Contractor agrees to maintain the confidentiality and security of the criminal justice history information in compliance with federal and state statutes, rules and regulations, and return or destroy such information when it is no longer needed to perform the Services contemplated herein.
- D. In the event that the Contractor's employee(s) fails to comply with the terms hereof, the Contractor shall take corrective action with the employee(s). Such corrective action must be acceptable to the Department. An intentional or knowing violation may also result in civil and criminal violations under federal and state laws. Additionally, the Contractor shall submit for the Department's approval, the Contractor's corrective action plan to ensure full compliance with the terms hereof. Until such time as the corrective action plan is approved by the Department, the Contractor shall not be authorized to fill any

vacant positions unless special authorization is granted in writing by the Department which authorization shall not be unreasonably withheld.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION H.6.

H.7 OTHER CONFIDENTIAL OR SENSITIVE INFORMATION

- A. The parties hereto acknowledge and agree that in order for the Contractor to perform the Services contemplated herein, the Department may have to provide the Contractor with, or the Contractor may have access to, certain information, other than criminal history information, that is confidential pursuant to federal or state laws, rules, or regulations, or that is personal information considered to be "sensitive." The Contractor agrees that such confidential or sensitive information shall only be used for the purpose of performing Services contemplated herein. Such information shall not be disclosed, copied or transmitted for any purpose other than for the performance of Services contemplated herein.
- B. In the event that the Contractor's employee(s) fails to comply with the terms hereof, the Contractor shall take corrective action with the employee(s). Such corrective action must be acceptable to the Department. An intentional or knowing violation may also result in civil and criminal violations under federal and state laws. Additionally, the Contractor shall submit for the Department's approval, the Contractor's corrective action plan to ensure full compliance with the terms hereof. Until such time as the corrective action plan is approved by the Department, the Contractor shall not be authorized to fill any vacant positions unless special authorization is granted in writing by the Department which authorization shall not be unreasonably withheld.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION H.7.

H.8 BOOKS AND RECORDS

All records and documents pertinent to the Services contracted hereunder shall be kept for a minimum seven (7) years after the expiration or termination hereof. If any litigation, claim, or audit involving these records begins before the retention period expires, the Contractor must continue to retain said records and documents until all litigation, claims, or audit findings are resolved, meaning that there is a final Court Order from which no further appeal may be made, or a written agreement is entered into between the Department and the Contractor.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION H.8.

H.9 ORGANIZATIONAL AND NAME CHANGE

The Contractor shall submit written notification to the Department within thirty (30) Days of any changes in the Contractor's name, address, telephone number, facsimile number and/or e-mail address with an effective date of such change. The Contractor shall submit to the Department a copy of any registration "to do business as," "OBA," or "also known as," "AKA," and any legal corporate name change filed with the Secretary of State.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION H.9.

H.10 FREE EXERCISE OF RELIGION

The Contractor is prohibited from substantially burdening an employee's or Offender's Free Exercise of Religion.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION H.10.

H.11 DELAY OF SERVICES

The Contractor shall meet its obligations to commence services at the facility within the time frames defined by the Contract. In the event the Contractor fails to meet those time frames as defined by the Contract, absent force majeure events and/or extensions from the Department, the Department will have the right to calculate reasonable revenues that are lost and charge the Contractor for each day the facility is inoperable due to delays caused by the Contractor's nonperformance (Exhibit J.4). The Department will provide written notification to the Contractor by certified mail, return receipt requested, of the charges which will include the date of imposition and the amount that was accrued daily as the date of the notification.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION H.11.

H.12 RESERVED FOR FUTURE USE

H.13 SECURITY

The Contractor's employees and representatives, vehicles and equipment must be under security surveillance at all times and are subject to inspection at any time while on state property. The Contractor agrees to abide by all Department Policies and unit rules and regulations on state property. These rules, in part, prohibit the introduction of alcohol, narcotics, weapons, gambling paraphernalia, pagers and cellphones to any state property. This includes having these items in personal vehicles of on-site employees. The Contractor's employees may not carry more than \$25.00 in cash into any Department Facility. Tobacco products are strictly prohibited on TDCJ units, but are allowed in the personal vehicles of on-site employees or in designated smoking

areas. All vehicles must be kept locked when not in use and the Contractor's employees must stay with the vehicle when it is unlocked.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION H.13.

SECTION I - CONTRACT CLAUSES**I.1 RESERVED FOR FUTURE USE****I.2 ADVERTISING OF AWARD**

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the products or services provided are endorsed or preferred by the Department or is considered by the Department to be superior to other products or services.

I.3 DEFAULT AND TERMINATION**I.3.1 DEFAULT BY CONTRACTOR**

Each of the following shall constitute an Event of Default on the part of the Contractor:

- A. A Material Failure to keep, observe, perform, meet, or comply with any covenant, agreement, term, or provision of this Contract to be kept, observed, met, performed, or complied with by the Contractor hereunder, when such failure continues for a period of twenty (20) Days after the Contractor's receipt of written notice thereof;**
- B. A Material Failure to meet or comply with Department Policy, federal or state requirement or law, when such failure continues for a period of twenty (20) Days after the Contractor's receipt of written notice thereof;**
- C. The Contractor's Material Failure to comply with any Department Policy for which the Contractor has been expressly required to comply and for which the Contractor has not received a prior written waiver from the Department, when such failure continues for a period of twenty (20) Days after the Contractor's receipt of written notice thereof;**
- D. Insolvency of the Contractor as evidenced by any of the following occurrences:**
 - 1. Its inability to pay its debts;**
 - 2. Any general assignment for the benefit of creditors;**
 - 3. Any decree or order appointing a receiver or trustee for it or substantially all of its property to be entered and, if entered without its consent, not to be stayed or discharged within sixty (60) Days;**
 - 4. Any proceedings under any law relating to bankruptcy, insolvency, or the reorganization or relief of debtors to be instituted by or against it**

and, if contested by it, not to be dismissed or stayed within sixty (60) Days; or

5. Any judgment, writ of attachment or execution, or any similar process to be issued or levied against a substantial part of its property which is not released, stayed, bonded, or vacated within sixty (60) Days after issue or levy.
- E. The discovery by the Department that any statement, representation or warranty in this Contract is false, misleading, or erroneous in any material respect; or
- F. A failure by the Contractor to comply with contractual terms and conditions, resulting in a breach of security or health and safety standards. This Event of Default may result in the immediate termination of this Contract.

I.3.2 Further Opportunity to Cure

- A. If an Event of Default of the type specified in Section 1.3.1 occurs and the Contractor reasonably believes that such Event of Default cannot be cured within the twenty (20) Days allowed in Section 1.3.1 but that such Event of Default can be cured through a diligent, on- going, and conscientious effort on the part of the Contractor, within a reasonable period not to exceed three (3) months, then the Contractor may, within the twenty (20) Day cure period, submit a detailed plan for curing the Event of Default to the Department.
- B. Upon receipt of any such plan for curing an Event of Default, the Department shall promptly review such plan and at its discretion, which must be reasonable in the circumstances, may allow, or not allow, the Contractor to pursue such plan of cure.
- C. The decision of the Department will be communicated in writing to the Contractor.
- D. The Department agrees that it will not exercise its remedies thereunder with respect to such Event of Default for so long as the Contractor diligently, conscientiously, and timely undertakes to cure the Event of Default in accordance with the approved plan.
- E. If the Department does not allow the Contractor an extension of the cure period, the twenty (20) Day time period shall be tolled during the period of time the request is pending before the Department.

I.3.3 Remedy of the Department

When an Event of Default by the Contractor has been determined to exist, the Department's Authorized Representative will notify, in writing, the Contractor of such

Event of Default, and subject to the provisions of Section 1.3.2, the Department will have the right to pursue any remedy it may have by law or in equity including, but not limited to:

- A. Reducing its claim to a judgment;
- B. Exercising a Termination for Default.
 - 1. In the event of Termination for Default the Department shall offset against Payments owed to the Contractor any reasonable amounts expended by the Department to cure the Event of Default.
 - 2. The Department will have no further obligations to the Contractor after such termination and the Contractor shall comply with Section H.3 with respect to the transition to new management.
 - 3. The Department may also acquire, in the manner the Department considers appropriate, services similar to those terminated and the Contractor will be liable to the Department for any increase in costs for those services.
 - 4. The Department shall not be liable for any increase in costs if the failure to perform the Contract arises from and without the fault or negligence of the Contractor as follows:
 - 1. Acts of God or of the public enemy,
 - 2. Acts of the State in either its sovereign or contractual capacity,
 - 3. Fires,
 - 4. Floods,
 - 5. Epidemics,
 - 6. Quarantine restrictions,
 - 7. Strikes,
 - 8. Freight embargoes, and
 - 9. Unusually severe weather.

In each instance the failure to perform must be beyond the control and without the fault or negligence of the Contractor.

I.3.4 RESERVED FOR FUTURE USE

I.3.5 RESERVED FOR FUTURE USE

I.3.6 Termination for Convenience

The Department may, in its sole discretion, terminate this Contract, with or without cause, by providing the Contractor with sixty (60) Days prior written notice of such termination.

I.3.7 Termination by Mutual Agreement

The parties may terminate this Contract by mutual agreement, the terms of which shall be set forth in writing.

I.3.8 Termination Procedures

A. Upon Termination for Default, Termination for Convenience, Termination by Mutual Agreement as heretofore mentioned, the following procedures will be adhered to:

- 1. The Department will immediately notify the Contractor in writing specifying the effective termination date.**
- 2. After receipt of the Notice of Termination, the Contractor shall immediately proceed with the following obligations, regardless of any delay in determining or adjusting any amounts due at that point in the Contract:**
 - a. Place no further subcontracts or orders in support of this Contract;**
 - b. Terminate all subcontracts; and c. Cancel all orders as applicable.**

B. Upon termination, the Department shall be entitled to receive from the Contractor, payment for all revenue owed under this Contract up to and including the date of termination.

The Department has no authority to reimburse a Contractor for capital equipment costs in the event that the Contract is terminated by mutual agreement or for cause before the expiration of the base period. Notwithstanding the foregoing, if the Contract is terminated prior to the end of the base period, the Department shall require any new service provider to compensate Contractor in an amount that equates to the undepreciated or unamortized portion of any equipment and infrastructure installed by Contractor which is used by the new service provider. In the event Contractor transfers ownership of or title to any equipment and infrastructure to the Department, including any equipment and infrastructure which become the property of the Department pursuant to the terms of this Contract, the compensation owed to the Contractor pursuant to the preceding sentence shall be calculated as if the ownership of such equipment and infrastructure had remained with Contractor and in accordance with an amortization/depreciation schedule to be provided by the Contractor to the Department at time of transfer of ownership of the equipment.

I.3.9 Default by the Department

Each of the following shall constitute an Event of Default on the part of the Department:

- A. Failure by the Department to observe and perform any material covenant, condition, or agreement on its part to be observed or performed; or**
- B. Its failure or refusal to substantially fulfill any of its material obligations hereunder, unless caused by the default of the Contractor; and**
- C. Unless cured by the Department within twenty (20) Days after receiving written notice thereof.**

I.3.10 Remedy of the Contractor

Upon an Event of Default by the Department, the Contractor's sole remedy shall be to follow the dispute resolution process in Section 1. 3.11 below.

I.3.11 Dispute Resolution

- A. Any dispute arising under this Contract, which is not disposed of by mutual agreement between the Department and the Contractor shall be resolved as follows:**
 - 1. The dispute resolution process provided for in Texas Government Code, Chapter 2260, shall be used, as further described herein, by the Department and the Contractor to attempt to resolve any claim for breach of Contract made by the Contractor.**
 - 2. A Contractor's claims for breach of this Contract that the parties cannot resolve in the ordinary course of business shall be submitted to the negotiation process provided in Texas Government Code, Chapter 2260, Subchapter B.**
 - 3. To initiate the process, the Contractor shall submit written notice, as required by Texas Government Code, Chapter 2260, Subchapter B, to the Contracts and Procurement Director or designee, at Two Financial Plaza, Suite 525, Huntsville, Texas 77340.**
 - 4. Said notice shall specifically state the provisions of Texas Government Code, Chapter 2260, Subchapter B, are being invoked, and shall also be given to all other representatives of the Department and the Contractor otherwise entitled to notice under the parties' Contract.**

5. Compliance by the Contractor with Subchapter B, is a condition precedent to the filing of a contested case proceeding under Texas Government Code, Chapter 2260, Subchapter C.
 6. The contested case process provided in Texas Government Code, Chapter 2260, Subchapter C, is the Contractor's sole and exclusive process for seeking a remedy for an alleged breach of Contract by the Department if the parties are unable to resolve their disputes under subparagraph (A) of this paragraph.
 7. Compliance with the contested case process provided in Texas Government Code, Chapter 2260, Subchapter C, is a condition precedent to sue from the Legislature under Chapter 107 of the Civil Practices and Remedies Code.
 8. Neither the execution of this Contract by the Department nor any other conduct of any representative of the Department related to the Contract shall be considered a waiver of sovereign immunity to suit.
- B. In addition to complying with Texas Government Code, Chapter 2260, the Department and the Contractor shall comply with the rule published in Texas Administrative Code, Title 37, Part 6, Chapter 155, Subchapter C, Rule 155.31.
- C. At all times during the course of the dispute resolution process, the Contractor shall continue with providing Services as directed, in a diligent manner and without delay, shall conform to the Department's directive, decision or order, and shall be governed by all applicable provisions of this Contract.
- D. Records of the Services performed shall be kept in sufficient detail to enable Payment in accordance with applicable provisions of this Contract, if this should become necessary.
- E. This provision shall not be construed to prohibit the Contractor from seeking any other legal or equitable remedy to which it is entitled.

I.4 NO WAIVER OF RIGHTS

- A. No failure on the part of any party to exercise, and no delay in exercising, and no course of dealing with respect to any right hereunder shall operate as a waiver thereof; nor shall any single or partial exercise of any right hereunder preclude any other or further exercise thereof or in the exercise of any other right.
- B. The remedies provided in this Contract are cumulative and non-exclusive of any remedies provided by law or in equity, except as expressly set forth herein.

I.5 INDEMNIFICATION OF THE DEPARTMENT

I.5.1 Acts or Omissions

The Contractor shall indemnify and hold harmless the State of Texas, the Department and the TBCJ, and/or their officers, agents, employees, representatives, contractors, assignees, and/or designees from any and all liability, actions, claims, demands, or suits, and all related costs, attorney fees, and expenses arising out of, or resulting from any acts or omissions of the Contractor or its agents, employees, subcontractors, order fulfillers, or suppliers of subcontractors in the execution or performance of the Contract and any purchase orders issued under the Contract. The defense shall be coordinated by the Contractor with the Office of the Attorney General when Texas State Agencies are named defendants in any lawsuit and the Contractor may not agree to any settlement without first obtaining the concurrence from the Office of the Attorney General. The Contractor and the Department agree to furnish timely written notice to each other of any such claim.

1.5.2 Infringements

- A.** The Contractor shall indemnify and hold harmless the State of Texas, the Department and the TBCJ, and or their employees, agents, representatives, contractors, assignees, and/or designees from any and all third party claims involving infringement of United States patents, copyrights, trade and service marks, and any other intellectual or intangible property rights in connection with the performances or actions of the Contractor pursuant to this Contract. The Contractor and the Department agree to furnish timely written notice to each other of any such claim. The Contractor shall be liable to pay all costs of defense including attorneys' fees. The defense shall be coordinated by the Contractor with the Office of the Attorney General when Texas State Agencies are named defendants in any lawsuit and the Contractor may not agree to any settlement without first obtaining the concurrence from the Office of the Attorney General.
- B.** The Contractor shall have no liability under this Section if the alleged infringement is caused in whole or in part by:
- 1.** Use of the product or Service for a purpose or in a manner for which the product or Service was not designed;
 - 2.** Any modification made to the product without the Contractor's written approval;
 - 3.** Any modification made to the product by the Contractor pursuant to the Department's specific instructions;
 - 4.** Any intellectual property right owned by or licensed to the Department;
or

5. Any use of the product or Service by the Department that is not in conformity with the terms of any applicable license agreement.
- C. If the Contractor becomes aware of an actual or potential claim, or the Department provides the Contractor with notice of an actual or potential claim, the Contractor may (or in the case of an injunction against the Department, shall), at the Contractors sole option and expense:
1. Procure for the Department the right to continue to use the affected portion of the product or Service; or
 2. Modify or replace the affected portion of the product or Service with functionally equivalent or superior product or Service so that the Department's use is non-infringing.

I.5.3 Taxes/Workers' Compensation/Unemployment Insurance - Including Indemnity

- A. The Contractor agrees and acknowledges that during the existence of this Contract, the Contractor shall be entirely responsible for the liability and payment of the Contractor's and the Contractor's employees' taxes of whatever kind, arising out of the performances in this Contract. The Contractor agrees to comply with all state and federal laws applicable to any such Persons, including laws regarding wages, taxes, insurance, and Workers' Compensation. The Department and/or the State shall not be liable to the Contractor, its employees, agents, or others for the payment of taxes or the provision of unemployment insurance and/or Workers' Compensation or any benefit available to a State employee or employee of another governmental entity customer.
- B. The Contractor agrees to indemnify and hold harmless the Department, the TBCJ, the State of Texas and/or their employees, agents, representatives, contractors, and/or assignees from any and all liability, actions, claims, demands, or suits, and all related costs, attorneys' fees, and expenses, relating to tax liability, unemployment insurance and/or Workers' Compensation in its performance under this Contract. The Contractor shall be liable to pay all cost of defense including attorneys' fees. The defense shall be coordinated by the Contractor with the Office of the Attorney General when Texas State Agencies are named defendants in any lawsuit and the Contractor may not agree to any settlement without first obtaining the concurrence from the Office of the Attorney General. The Contractor and the Department agree to furnish timely written notice to each other of any such claim.

I.6 NO WAIVER OF DEFENSES

- A. Neither the Department nor the Contractor shall waive, release or otherwise forfeit any possible defense the Department or the Contractor may have

regarding claims arising from or made in connection with the performance of the Services by the Contractor without the consent of the other party.

- B. The Department and the Contractor shall reserve all such available defenses and cooperate with each other to make such defenses available for each other's benefit to the maximum extent allowed by law, including any defenses the Department may have regarding litigation, losses and costs resulting from claims or litigation pending at the time the Contract becomes effective, or arising thereafter from occurrences prior to the effective date hereof.

I.7 INDEPENDENT CONTRACTOR

- A. The Contractor is associated with the Department only for the purposes and to the extent set forth herein, and with respect to the performance of Services hereunder, the Contractor is and shall be an independent contractor and shall have the sole right to supervise, manage, operate, control, and direct the performance of the details incident to its duties hereunder.
- B. Nothing contained herein shall be deemed or construed to create a partnership or joint venture, to create the relationships of an employer-employee or principal-agent, or to otherwise create any liability for the Department whatsoever with respect to the indebtedness, liabilities, and obligations of the Contractor or any other party.
- C. The Contractor shall be solely responsible for (and the Department shall have no obligation with respect to) payment of all Federal Income, FICA, and other taxes owed or claimed to be owed by the Contractor, arising out of the Contractor's association with the Department pursuant hereto, and the Contractor shall indemnify and hold the Department harmless from and against any and all liability from all losses, damages, claims, costs, penalties, liabilities, and expenses howsoever arising or incurred because of, incident to, or otherwise with respect to any such taxes.

I.8 LAWS OF TEXAS

This Contract shall be governed by and construed in accordance with the laws of the State of Texas. The venue of any suit arising under this Contract is fixed in any court of competent jurisdiction of Travis County, Texas.

In the event of a conflict between the Contract and the State laws of Texas, the laws shall prevail. If there is no conflict between the laws and the Contract, the requirements most favorable to the Department shall prevail.

I.9 ASSIGNMENT

- A. The Contractor may not assign any interest in this Contract without the prior written consent of the Department which consent the Department may withhold at its sole discretion.**
- B. If the Department so elects in its sole discretion, this Contract will terminate upon the occurrence of any of the following:**
 - 1. More than fifty percent (50%) of the assets of the Contractor are sold;**
 - 2. The Contractor is merged into, acquired by, or consolidated with another corporation or business entity; or is otherwise the subject of reorganization; or**
 - 3. Any shareholder or owner of the Contractor who owns at least ten percent (10%) beneficial ownership of the Contractor fails to continue to own at least ten percent (10%).**
- C. In the event that any sale, transfer, or assignment, as referenced in paragraphs A and B above, is consented to by the Department, the transferee or its legal representative shall agree in writing with the Department to assume, perform and be bound by the covenants, obligations and agreements contained herein.**

I.10 MAINTENANCE OF CORPORATE EXISTENCE AND BUSINESS

- A. The Contractor, if incorporated, shall at all times maintain its corporate existence and authority to transact business and be in good standing in its jurisdiction of incorporation and the State of Texas.**
- B. The Contractor shall maintain all licenses, permits and franchises necessary for its businesses where the failure to so maintain might have a material adverse effect on its ability to perform its obligations under this Contract.**

I.11 APPROVAL OF CONTRACT

- A. This Contract is subject to written approval of the Executive Director of the Department and shall not be binding until so approved.**
- B. For Contracts valued over \$1,000,000 in the initial Contract Term, the Executive Director's approval shall be given only on the approval of the TBCJ.**

I.12 NON-DISCRIMINATION

In the performance of this Contract, the Contractor warrants that it shall not discriminate against any employee, subcontractor, participant or provider on account

of race, color, disability or perceived disability, religion, sex, national origin, genetic information or age, and in accordance with the following :

- A. The Contractor shall not discriminate against employees, subcontractors, participants or providers who have or are perceived to have a disability because AIDS/HIV infection, antibodies to HIV, or infection with any other probable causative agent of AIDS. The Contractor shall post notices setting forth the provisions of this Non-Discrimination Clause in conspicuous places, available to employees and applicants for employment.
- B. In all solicitations or advertisements for employees and/or the purchase of Services, the Contractor shall state that it is an equal opportunity employer; provided, however, that notices, advertisements and solicitations placed in accordance with federal law, rule or regulation shall be deemed sufficient for the purpose of meeting this requirement.
- C. The Contractor shall include the provisions of the foregoing paragraphs in every subcontract so that such provisions shall be binding upon each subcontractor or vendor.

I.13 CONFIDENTIALITY AND OPEN RECORDS

I.13.1 Confidentiality

Any confidential information provided to or developed by the Contractor in the performance of the Contract shall be kept confidential unless otherwise provided by law and shall not be made available to any individual or organization by the Contractor or the Department without prior approval of the other party.

I.13.2 Open Records

In accordance with Texas Government Code, Section 2252.907, the Contractor acknowledges that this Contract and information created or maintained in connection with this Contract is public information and subject to disclosure as provided by Texas Government Code, Chapter 552 (Texas Public Information Act). The Texas Public Information Act may require the Contractor to make information related to this Contract available to the public pursuant to a request for public information. The Contractor agrees, upon request, to make information related to this Contract that is not otherwise excepted from release by the Texas Public Information Act available to the public in hard copy, unless the requester of the information consents to receive the information in another mutually agreeable format. The Contractor acknowledges that the agency shall not provide legal counsel related to the Contractor's compliance with the Texas Public Information Act.

I.14 CONTRACT CHANGES

- A. Changes/modifications to this Contract (except Contract extensions in accordance with Sections 1. 15 and 1. 16; administrative changes, such as changing the Contract Specialist designation or correcting typographical errors; or other unilateral changes discussed elsewhere in the Contract) shall be mutually agreed to by the parties and executed in writing with the authorized signatures .**
- B. The Department, at its sole discretion, may revise funding during the course of this Contract by issuing a unilateral modification to the Contractor.**

I.15 OPTION TO EXTEND THE TERM OF THE CONTRACT

- A. The Department may, at its sole discretion, extend the Contract Term by written notice to the Contractor within ten (10) Days of Contract expiration, provided that the Department shall give the Contractor a preliminary written notice of its intent to extend at least sixty (60) Days before the Contract expires.**
- B. The preliminary notice does not commit the Department to an extension.**
- C. If the Department exercises this option, the extended Contract shall be considered to include this option provision.**

I.16 OPTION TO EXTEND SERVICES

- A. The Department may require continued performance of any Services within the limits and at the rates specified in this Contract.**
- B. The Department reserves the right to extend this Contract for a ninety (90) Day period at the end of each Contract and/or extension period for the purpose of re-advertising the Service, awarding a new Contract, and transitioning into a new Contract.**
- C. This option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed six (6) months.**
- D. The Department may exercise the option by written notice to the Contractor within the period specified in Section 1.15.**

I.17 SEVERABILITY

In the event that any provision of this Contract is later determined to be invalid, void, or unenforceable, then the remaining terms, provisions, covenants, and conditions of this Contract shall remain in full force and effect, and shall in no way be affected, impaired, or invalidated.

I.18 IMMIGRATION

The Contractor represents and warrants that it will comply with the requirements of the Immigration and Nationality Act (8 U.S.C. Section 1101 et seq.) and all subsequent immigration laws and amendments.

I.19 NO LIABILITY UPON TERMINATION

If this Contract is terminated for any reason, the Department and the State of Texas shall not be liable to the Contractor for any damages, claims, losses, or any other amounts arising from or related to any such termination. However, the Contractor may be entitled to the remedies established in Section 1.3.11.

I.20 LIMITATION ON AUTHORITY

The Contractor shall have no authority to act for or on behalf of the Department or the State of Texas except as expressly provided for in this Contract; no other authority, power or use is granted or implied. The Contractor may not incur any debts, obligations, expenses, or liabilities of any kind on behalf of the State of Texas or the Department.

I.21 INTELLECTUAL PROPERTY INDEMNIFICATION

- A. The Contractor will indemnify, defend, and hold harmless the State of Texas and the Department against any action or claim brought against the State of Texas and/or the Department that is based on a claim that software infringes any patent rights, copyright rights or incorporated misappropriated trade secrets. The Contractor will pay any damages attributable to such claim that are awarded against the State of Texas and/or the Department in a judgment or settlement.**
- B. If the Department's use of the software becomes subject to a claim, or is likely to become subject to a claim, in the sole opinion of the Department, the Contractor shall, at its sole expense (1) procure for the Department the right to continue using such software under the terms of this Contract; or (2) replace or modify the software so that it is non-infringing.**

I.22 ELECTRONIC AND INFORMATION RESOURCES ACCESSIBILITY STANDARDS, as required by Texas Administrative Code, Title 1, Part 10, Chapter 213

- A. Effective September 1, 2006 State Agencies and Institutions of Higher Education shall procure products which comply with the State of Texas Accessibility requirements for Electronic and Information Resources specified in Texas Administrative Code, Title 1, Part 10, Chapter 213, when such products are available in the commercial marketplace or when such products are developed in response to a procurement solicitation.**

- B. The Contractor shall provide the Department with the URL to its Voluntary Product Accessibility Template (VPAT) for reviewing compliance with the State of Texas Accessibility requirements (based on the federal standards established under the Rehabilitation Act, Section 508), or indicate that the product/service accessibility information is available from the General Services Administration "Buy Accessible Wizard" (<http://www.buyaccessible.gov>). Contractors not listed with the "Buy Accessible Wizard" or supplying a URL to their VPAT must provide the Department with a report that addresses the same accessibility criteria in substantively the same format. Additional information regarding the "Buy Accessible Wizard" or obtaining a copy of the VPAT is located at <http://www.section508.gov/>.

I.23 RIGHTS TO DATA, DOCUMENTS AND COMPUTER SOFTWARE (STATE OWNERSHIP)

Any software, research, reports, studies, data, photographs, negatives or other documents, drawings or materials prepared by the Contractor in the performance of its obligations under this Contract shall be the exclusive property of the State of Texas and all such materials shall be delivered to the Department by the Contractor upon completion, termination, or cancellation of this Contract. The Contractor may, at its own expense, keep copies of all its writings for its personal files. The Contractor shall not use, willingly allow, or cause to have such materials used for any purpose other than the performance of the Contractor's obligations under this Contract without the prior written consent of the Department; provided, however, that the Contractor shall be allowed to use non-confidential materials for writing samples in pursuit of the work. The ownership rights described herein shall include, but not be limited to, the right to copy, publish, display, transfer, prepare derivative works, or otherwise use the works.

I.24 FORCE MAJEURE

- A. Neither the Contractor nor the Department shall be liable to the other for any delay in, or failure of performance, of any requirement included in this Contract caused by force majeure. The existence of such causes of delay or failure shall extend the period of performance until after the causes of delay or failure have been removed provided the non-performing party exercises all reasonable due diligence to perform.
- B. Force majeure is defined as acts of God, war, fires, explosions, hurricanes, floods, failure of transportation, or other causes that are beyond the reasonable control of either party and that by exercise of due foresight such party could not reasonably have been expected to avoid, and which, by the exercise of all reasonable due diligence, such party is unable to overcome.
- C. Each party must inform the other in writing, with proof of receipt, within three (3) working days of the existence of such force majeure, or otherwise waive this right as a defense.

I.25 NOTICES

Any written notices required under this Contract will be delivered by carrier service to the Contractor's office address specified on Page 1 of this Contract or by U.S. mail.

Notices to the Department shall be sent to:

**Terri Bennett, CTPM, CTCM
Contract Specialist
Texas Department of Criminal Justice
Contracts and Procurement Department
Information Technology, Construction and Utilities Branch
Two Financial Plaza, Suite 525
Huntsville, Texas 77340**

Notice will be effective on receipt by the affected party. Either party may change the designated notice address in this Section by written notification to the other party. This change shall be incorporated with a unilateral modification.

1.26 SUBSTITUTIONS

Substitutions are not permitted without written approval of the Department.

1.27 U.S. DEPARTMENT OF HOMELAND SECURITY'S E-VERIFY SYSTEM

- A. By entering into this Contract, the Contractor certifies and ensures that it utilizes and will continue to utilize, for the term of this Contract, the U.S. Department of Homeland Security's E-Verify system to determine the eligibility of:**
- 1. All Persons employed to perform duties within Texas, during the Contract Term; and**
 - 2. All Persons (including subcontractors) assigned by the Contractor to perform work pursuant to the Contract, within the United States of America.**
- B. The Contractor shall provide, upon request of the Department, an electronic or hardcopy screenshot of the confirmation or tentative non-confirmation screen containing the E-Verify case verification number for attachment to the Form 1-9 for the three (3) most recent hires that match the criteria above, by the Contractor, and the Contractor's subcontractors, as proof that this provision is being followed.**
- C. If this certification is falsely made, the Contract may be immediately terminated, at the discretion of the State and at no fault to the State, with no prior notification. The Contractor shall also be responsible for the costs of any**

re-solicitation that the State must undertake to replace the terminated Contract.

CENTURYLINK HAS READ, UNDERSTANDS, AND WILL COMPLY WITH EACH ITEM OUTLINED IN SECTION I

ATTACHMENTS

Attachment F:
Preliminary Implementation Plan

Attachments G:
Quality Control Plan

Attachment H
Sample SCP Reports

ATTACHMENT F: PRELIMINARY IMPLEMENTATION PLAN

ID	Task Name	Duration	Start	Finish
1	CenturyLink Offender Calling System Installation Project Plan for Texas Department of Criminal Justice	191 days	Tue 9/4/18	Tue 5/28/19
2	Offender Calling System Installation & Cut-Over	191 days	Tue 9/4/18	Tue 5/28/19
3	Project Initiation Phase	6 days	Tue 9/4/18	Tue 9/11/18
4	On Site Kick-Off meeting with TDCJ & CenturyLink Account Team	3 days	Tue 9/4/18	Thu 9/6/18
5	Site Surveys conducted by CenturyLink Field Services Team (Mandatory)	3 days	Fri 9/7/18	Tue 9/11/18
6	Project Planning Phase	71 days	Thu 9/13/18	Thu 12/20/18
7	Engineering Schematics, Bill of Materials, and Manual of Procedure (MOP) Updates	7 days	Thu 9/13/18	Fri 9/21/18
8	Agency Provisioning and Data Management	55 days	Mon 9/24/18	Fri 12/7/18
9	Product and feature provisioning within the operational platforms	70 days	Fri 9/14/18	Thu 12/20/18
10	Hardware and LEC transport orders	14 days	Fri 9/14/18	Wed 10/3/18
11	Project Execution Phase	137 days	Fri 10/5/18	Mon 4/15/19
12	Delivery confirmations	82 days	Fri 10/5/18	Mon 1/28/19
13	LEC Circuit deliveries (As Necessary)	70 days	Fri 10/5/18	Thu 1/10/19
14	Hardware deliveries throughout DOC	68 days	Thu 10/25/18	Mon 1/28/19
15	Pre-Installation activities per facility	67 days	Mon 11/19/18	Tue 2/19/19
16	Verification of shipment content to pick list	66 days	Mon 11/19/18	Mon 2/18/19
17	Process received hardware paperwork	66 days	Tue 11/20/18	Tue 2/19/19
18	Installation activities per facility	99 days	Wed 11/21/18	Mon 4/8/19
19	Installation of all required hardware in phone room and through the facility	96 days	Wed 11/21/18	Wed 4/3/19
20	Installation of all phones by pod or dorm	98 days	Thu 11/22/18	Mon 4/8/19
21	Installation of additional workstations	96 days	Fri 11/23/18	Fri 4/5/19
22	Installation of Video Visitation at designated 12 locations	96 days	Fri 11/23/18	Fri 4/5/19
23	Training of product and feature utilities	15 days	Tue 3/26/19	Mon 4/15/19
24	Walkthrough of product details by user group access	15 days	Tue 3/26/19	Mon 4/15/19
25	Agency training certifications by user group	15 days	Tue 3/26/19	Mon 4/15/19
26	Controlling and Monitoring Phase	104 days	Wed 12/5/18	Mon 4/29/19
27	Perform Change checkpoints	90 days	Wed 12/19/18	Tue 4/23/19
28	Identify change orders for specific facility requirements not identified at Site Survey	90 days	Wed 12/19/18	Tue 4/23/19
29	Quality evaluation checkpoints	104 days	Wed 12/5/18	Mon 4/29/19
30	Verification of project installation activity by facility	104 days	Wed 12/5/18	Mon 4/29/19
31	Complete checklists and document connectivity and utilization per facility	104 days	Wed 12/5/18	Mon 4/29/19
32	Closing Phase	34 days	Thu 4/11/19	Tue 5/28/19
33	Cutover of product and features to calling platform	19 days	Thu 4/11/19	Tue 5/7/19
34	Reverification of services are functional	15 days	Thu 4/11/19	Wed 5/1/19

ID	Task Name	Duration	Start	Finish
35	Cut sheet distribution	4 days	Thu 5/2/19	Tue 5/7/19
36	Post cutover activities	15 days	Wed 5/8/19	Tue 5/28/19
37	Open project tickets for post cutover monitoring	15 days	Wed 5/8/19	Tue 5/28/19
38	Monitor site activities of product functionality	15 days	Wed 5/8/19	Tue 5/28/19
39	Agency acceptance and project closure	15 days	Wed 5/8/19	Tue 5/28/19

ATTACHMENT G QUALITY CONTROL PLAN

**CENTURYLINK
OFFENDER TELEPHONE & RELATED
SERVICES
TEXAS DEPARTMENT OF CRIMINAL
JUSTICE**

QUALITY CONTROL PLAN

MAY 23, 2018

PREFACE

The ability to quantify and measure objectives provides both the Department and the CenturyLink Team with the necessary information to ensure that they are met. In this section we address the Quality Control Plan and the tools to quantify and measure the objectives of the Department.

Accurate and thorough assessments of each of the Departments expectations, and how we can meet those expectations, are critical to our continued success. In most instances specific performance measures or service standards are results of a combination of the proposal, contract commitments, meeting industry standards and specific customer requests and requirements. The purpose of this document to identify the performance measures and action plans which enable the CenturyLink Team to provide the highest quality service, applications and features.

The CenturyLink Team's Service Organization assumes responsibility for this document and updates it, as required, to meet the needs of the Department. Users of this document may report deficiencies or corrections using the Document Change Request found at the end of the document. Updates to this document will be performed, at least annually.

SECTION 1: INTRODUCTION

1.1 Purpose

The purpose of this plan is to define the Offender Telephone System for the Departments Quality Control (QC) including tasks and responsibilities and to provide reference documents and guidelines to perform the QC activities; provide the standards, practices and conventions used in carrying out QC activities; and provide the tools, techniques, and methodologies to support QC activities, and reporting.

1.2 Document Overview

This document identifies the organizations and procedures to be used to perform activities related to the TDCJ QC program:

Section 1 Introduction and Quality Control Plan Application including an overview of the system

Section 2 Organizational Responsibilities

Section 3 Organization Quality Metrics

Section 4 Quality Plan Objectives and Methodologies

Section 5 Quality Plan Monitoring Process

1.3 System Overview

Secure Call Platform (SCP)

The first step in any QC plan is a calling architecture that inherently maximizes feature quality and reliability. As discussed in Section L requirement 1, this reliability is one of SCP's unique advantages and derives from its centralized, fully redundant capabilities and digitally clear transport method.

Carrier-Class Centralized Architecture:

Virtually eliminates on-site equipment, easing operation and reducing downtime

- Expedites installation due to fewer components and no elimination of on-site "tuning"
- Reduces maintenance problems; fewer visits to the site
- Improves time-to-repair; no "windshield" time needed for system break-fix
- Provides a carrier-class physical environment for equipment
- Ensures call records are backed up in real-time, rather than through a nightly batch process
- Provides one, centralized platform for faster service delivery
 - Delivers a single platform for focused new service development; no need to manage multiple software versions
 - Enables software updates/upgrades to occur simultaneously across all facilities
- Facilitates system expansion; additional sites are turned up with "flip of a switch"
- Consolidates all communications (voice and data) into a single network

- Speeds provisioning time
- Simplifies network management, speeding fault isolation
- Improves security through encrypted transmission

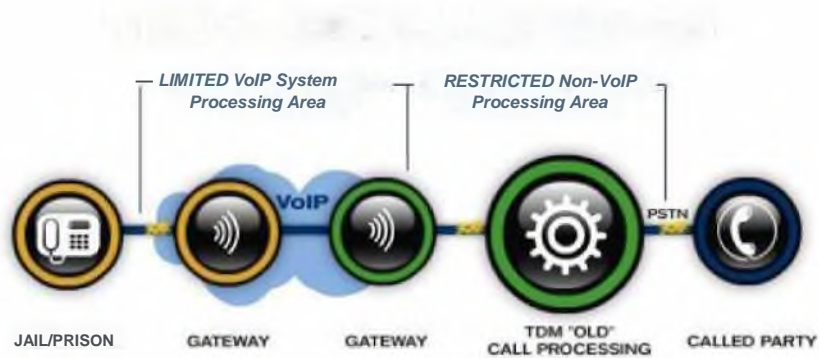
Digital Transport:

Analog transport systems can be slow and prone to noise and static interruptions. The effect on a phone conversation is oftentimes, garbled conversations.

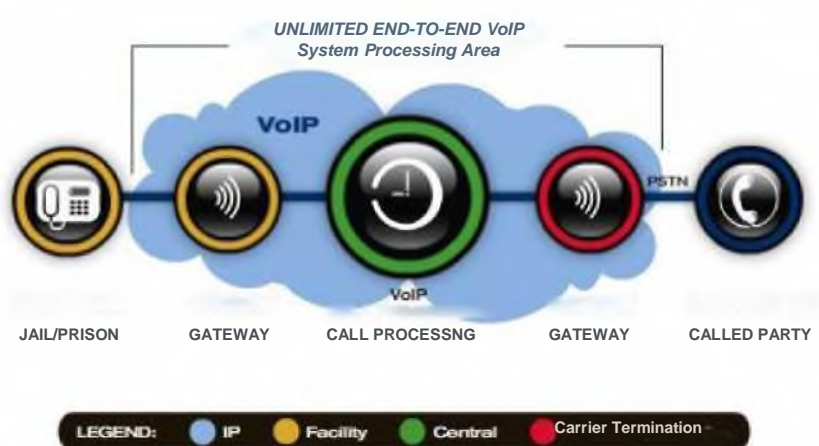
SCP's fully digital system provides clear delivery across the entire call-processing network. Digital transport is an extremely efficient means of moving data, and the more efficient a system is at moving data, the faster it gets to its destination and the "cleaner" the data remain. Benefits include:

- High-quality recordings, allowing investigators to easily discern key words as well as suspicious background sounds in both the offender's and the called party's environment
- Reduced complaints due to poor sound quality
- Improved effectiveness of the OTS to detect and prevent fraudulent activity, such as 3-way calling attempts

TRADITIONAL PROVIDERS



SECURE CALL PLATFORM



SECTION 2: ORGANIZATIONAL RESPONSIBILITIES

The following are the major functional groups that influence the quality of the OTS with a brief description of the primary role each plays in delivering service, features and applications.

2.1 Sales and Marketing

Sales and Marketing identifies customer needs and requirements and matches services and solutions to those needs. Clearly articulates the proposed solution to each customer and gains their complete approval through contractual commitments and other supporting documentation. Identifies new customer requirements and provides them to Product Management for evaluation.

2.2 Product Management

Product Management is an organizational function within the CenturyLink Team dealing with our products at all stages of the product lifecycle including the proposed OTS. The core activities of the product management organization include; defining new products, gathering market requirements and building product roadmaps, particularly technology roadmaps.

2.3 Information Technology

The CenturyLink Team Information Technology (IT) departments are responsible for design, development, implementation, support or management of computer-based information systems, particularly software applications and computer hardware which are the functional components of the CenturyLink Team's OTS. Our IT uses computers and computer software to convert, store, protect, process, transmit, and securely retrieve information.

2.4 Engineering

The CenturyLink Team's Engineering organization is responsible for building the best possible OTS solution for the Department. Based upon comprehensive facility location surveys as well as input from the customer and the sales organization, this group identifies all required equipment and network telecom facilities required to provide a comprehensive solution to each customer.

2.5 Telecom Services

Telecom Services is responsible for identifying the telecommunications network requirements for all facilities, placing orders for all required telecommunications and following up with the carriers to ensure the service is delivered to the correct location in time to meet the schedule of the Implementation Plan.

2.6 Support Systems Management

Support Systems Management is responsible for ongoing management and quality control for critical non-billing systems not inherent in the OTS. These include management of IVR systems for offenders and/or the public (if desired), auto dialer callouts in the case of an emergency, and even commissioning database support.

2.7 Installation

There will be multiple installation teams dedicated to installing the OTS. These installation teams will be led by dedicated project managers who have the overall responsibility for the execution of the Implementation Plan.

2.8 Technical Support

Technical Support is responsible for receiving OTS issues for customers and members of the CenturyLink Team, opening a trouble ticket in the HEAT system, responding back to the customer with confirmation that the issue is being work by the technical support staff, troubleshooting the issue and taking the appropriate corrective action and confirming with the customer that the issue has been resolved to their satisfaction.

2.9 Network Operations

Network Operations Center (NOC) proactively monitors all of the network components and systems used to provide service to the Departments facilities. Any activity outside of normal operating parameters is logged into the HEAT and is immediately investigated.

2.10 Billing Operations

Billing Operations is responsible for gathering the billing information associated with each site, applying the specific rate table to the calls made from the offender telephones and formatting the billing information in the exact form required by the billing method selected by the end user.

2.11 Rates & Regulatory

Rates and Regulatory confirms that rates comply with the requirements of all tariffs and that all other government regulations are being stringently followed.

2.12 Field Maintenance

Field Technicians perform routine maintenance on the telephone and equipment at TDCJ facilities as well as responding to specific trouble reports. Service Representatives provide administrative support to facilities and are responsible for resolving offender complaints, updating offender calling lists and managing biometric enrollments.\

2.13 Securus Correctional Billing Services (SCBS)

Provides account establishment, account management and billing customer service to the friends and families of offenders. Securus Correctional Billing Service has in-house trained customer service specialists on staff to handle customer calls 7 days a week, 24 hours per day. In addition, customers may also use a web based customer service portal or check balances or fund accounts with our automated telephone support system featuring a state of the art (Integrated Voice Response) system.

2.14 Finance and Accounting

Finance and Accounting are responsible for providing the funding for the initial installation, monitoring the revenue performance and the integrity of the revenue reporting from TDCJ facilities. This group is responsible for accumulating revenue information on a monthly basis and calculating an accurate commission payment for TDCJ and sending the commission payment and a report detailing the underlying usage to TDCJ on time each month.

2.15 Training

The CenturyLink Training Team is responsible for initial and follow-up training. Training will be available on site during the initial implementation. Follow-up training for system enhancements of for new employees will be scheduled based upon the needs to the Departments.

2.16 Customer Satisfaction

The Customer Satisfaction Team is a completely independent group which acquires direct customer feedback and measures customer satisfaction on scheduled and incidental basis. This group compiles all of the customer surveys and distributes the information to all departments and to senior management. The Director of Customer Satisfaction Team leads the Improvement Opportunity Team which is tasked with addressing identified service or product issues at the individual customer level.

SECTION 3: ORGANIZATIONAL QUALITY METRICS

Metrics are obtained through a variety of methods. A primary source of feedback for each group is the annual Customer Satisfaction survey (refer to Attachment I - Customer Surveys). This survey gives customers the opportunity to numerically rate our performance on dozens of objectives, and provide subjective feedback through several open-ended questions. Portions of this survey particularly relevant to each group are presented below, noting that written comments are also scrutinized to understand root cause and drive corrective action with the appropriate group.

3.1 Sales/Account Management & Marketing

The quality metrics for the Sales and Marketing have both an internal and external component each of which is critical to the success of the Departments OTS project.

The primary sales metric is 100% sales order accuracy. One of the processes of the CenturyLink Team are driven by is the accuracy of the sales order. It is internal representation of the specific agreement between Department and the CenturyLink Team. This is a mechanized process that Account Management uses to document all customer requirements and, along with the implementation plan developed from site surveys conducted by our installation team, is the backbone of delivering the OTS.

It is also critical that we understand the Department's opinion of the performance of all of the members of the CenturyLink Team. On an annual basis our Customer Satisfaction Group surveys each customer to determine how they believe the CenturyLink Team is performing. The following are the specific elements we ask our customers to measure for the sales team. Our objective for these metrics is an overall score of 9, with remedial action immediately taken for scores less than 7.

CenturyLink

CenturyLink Public Communications Customer Experience Questionnaire

Business Value

Please indicate your level of satisfaction with CenturyLink Public Communications in each of the following areas:

	⇐ Not at all Satisfied					Extremely Satisfied ⇐					
	0	1	2	3	4	5	6	7	8	9	10
Ability to meet expectations	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Solution meets your business needs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Trusted business relationship	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Overall Performance

Please rate your level of satisfaction with your [Account Manager](#) (Donna Ivey) in each of the following areas:

	⇐ Not at all Satisfied					Extremely Satisfied ⇐					
	0	1	2	3	4	5	6	7	8	9	10
Anticipates/recommends solutions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Frequency of communications	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Responds in a timely manner	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Effectiveness at facilitating issue resolution	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

We welcome any additional feedback related to your [Account Manager](#):

1500 characters left.

3.2 Product Management

It is essential that Product Management communicate all of the functional requirements of new applications to the development team and to the Sales and Service teams. An important metric for successful performance is the complete accuracy in the description of functional requirements and the successful communication of those requirements. A second critical metric is the on-time delivery of features and applications that completely meet requirements within the scheduled timeframes.

3.3. Information Technology

Overall call processing performance of the OTS is the primary responsibility of Information Technology team, including measured system availability, processing speed, and OTS data accuracy. The introduction of new applications and features must be accomplished through thoroughly tested implementation protocols and without an interruption in the existing functionality of the OTS.

3.4 Engineering

Engineering must accurately identify all required equipment and network telecom facilities required. They are required to develop a meticulously accurate Build of Materials (BOM) and the identification of the scope of network facilities required to ensure a successful implementation plan.

3.5 Telecom Services

Accurately order and deliver all required telecommunications services needed provision the OTS at each and every facility. 100% order accuracy and delivery is the standard metric for Telecom Services.

3.6 Support Systems Management

Each system supported by this group has individual associated performance metrics. For IVR systems, availability, blocked call attempts, and redials within 24 hours are checked daily for 1-2 weeks before reducing checks to a weekly process. For auto dialer management, request receipts are logged and compared to the time of initial and final call attempt. For commissioning database support, success is measured by the timeliness of commissions paid.

3.7 Installation

Meeting the scheduled end completion date is a critical quality metric for the Installation Teams. The comprehensive Implementation Plan identifies all of the metric components which will drive the successful completion of the project and is the guiding force and measurement tool for the Installation team. Each site will also be asked to provide their evaluation of the performance of the CenturyLink Team based upon the following survey:

Please rate your level of satisfaction with the following aspects of your Implementation:

	<= Not at all Satisfied					Extremely Satisfied =>					
	0	1	2	3	4	5	6	7	8	9	10
Scope of work was clearly defined	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Project plan clearly outlined key milestones and dates	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Proactive status updates provided throughout the implementation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Knowledge/expertise of resources	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Professional and courteous staff	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
All features and functionality delivered as promised during RFP process	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Solution meets your business needs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Time to complete met your expectations	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Were you introduced to your Program Manager (donna.pivey@centurylink.com) who will serve as your main point of contact for any service related questions and/or issues going forward?

Yes No

We welcome any additional feedback regarding your Implementation experience.

1500 characters left.

An overall score of 9 is the benchmark/objective for a successful installation, and any individual score of 7 of less is considered unacceptable and immediate corrective active action is initiated.

3.8 Technical Support

Technical support is a highly measured function, with objectives driven by meeting service level commitments that are specific for the requirements of the Department, including initial response time, time to resolution, and frequency of repeat problems. The following is an example of the tracking that will be used to ensure we are meeting our Department commitments:

Priority	Ticket Number	Initial # Tickets Non-Compliant	Initial Percent Compliant	Corrected# Tickets Non-Compliant	Corrected Percent Compliant
1	28	5	82.14%	0	100.00%
2	3	0	100.00%	0	100.00%
3	2	0	100.00%	0	100.00%
4	55	0	100.00%	0	100.00%
5	4724	0	100.00%	0	100.00%

1-4	88	5	94.32%	0	100.00%
5	4724	0	100.00%	0	100.00%
Total	4812	5	99.90%	0	100.00%

Additionally we will solicit TDCJ feedback on the level of service provided through the Customer Experience Questionnaire.

3.9 Network Operations

Network Operations is also a highly measured function, with metrics including network availability, transmission latency, performance of peripheral equipment, and the overall availability of the OTS.

3.10 Billing Operations

We are highly sensitive to the need for accurate customer billing and have independent groups who perform regular collect and prepaid collect test calls to ensure billing and rating accuracy. In addition, we perform monthly audits of call detail records to ensure each call was rated at the proper rates per the contract.

Critical metrics for Billing Operations include accurate application of rates, delivering accurate and timely billing information to each of the billing applications supported by the CenturyLink Team, and providing accurate billing and revenue information are the critical metrics for Billing Operations.

3.11 Rates & Regulatory

The critical metric for Rates and Regulatory are one hundred percent compliance with call rates and local, state and federal tariffs.

3.12 Field Service & Maintenance

Field Technicians are responsible for meeting Department requirements for service level commitments when a dispatch is required. Service Representatives and Field Technicians both have expected levels of production for routine maintenance and for administrative activities required to provide the OTS service to the Department.

Measures of technician performance are calculated and stored within the trouble ticketing system, and include troubles per 100 phones managed, repeated troubles, time to respond, and time to restore.

In addition to these measures, the following survey information is solicited from our customers with regard to field technician performance:

CenturyLink

CenturyLink Public Communications Customer Experience Questionnaire

Overall Performance

Please rate your level of satisfaction with your Administrator/ Field Technician (Donna Ivey) in each of the following areas:

	<= Not at all Satisfied					Extremely Satisfied >=					
	0	1	2	3	4	5	6	7	8	9	10
Responds to ticket requests for onsite support in a timely manner	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Proactive status updates on open issues	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Courteous and professional while onsite	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Has knowledge/tools necessary to effectively service your account	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

We welcome any additional feedback related to your Administrator/ Field Technician.

1500 characters left.

3.13 Securus Correctional Billing Services (SCBS)

It is crucial to operating an OTS system that friends and families are able to establish telephone accounts and to quickly and easily have any questions and concerns addressed. key metrics for SCBS include, the availability of customer service representatives as measured by hold time before reaching a representative and resolution time as measured by the amount of time required by the customer service representative to handle the customers calls. The following automated telephone survey is used to evaluate the effectiveness of the customers experience with SCBS:

Questions
Q1. The hold time I experience while attempting to reach a customer service representative was satisfactory.
Q2. The customer service representative was professional and courteous throughout the call.
Q3. Customer Service representative understand and answered my question(s) accurately.
Q4. The customer service representative resolved my issue on this call within company policy.
Q5. The Phone System was easy to use.
Q6. I found Securustech.net website helpful and will continue to use it in the future.
Q7. Please provide additional feedback (Optional):

Q8. What was most helpful to you on the Securustech.net website?

Q9. Did you experience any difficulty using the Securustech.net website?

Q10. Securus made it easy for me to handle my issue.

The CenturyLink Team will also solicit the input of the Department regarding the performance of the SCBS organization through our Customer Satisfaction Surveys.

3.14 Finance & Accounting

Finance and Accounting metrics for the Department will be 100% accuracy of all revenue information used to calculate commissions, 100% on time performance in delivering commission payments and commission reports, and 100% successful compliance with all audits.

3.15 Training

The performance metrics for facility training include the timely delivery of training, the relevance of the course content to the group which is being trained and the value the training had for the facility. The measure of timeliness has been established in the RFP. Post course completion surveys will be used to determine the validity of the course content and the value of the training including the method it was delivered.

3.16 Customer Satisfaction

A performance metric for Customer Satisfaction is to survey 100% of the Department's facilities annually for overall satisfaction and value assessment. This group will also use the data for all of the CenturyLink Team's surveys to identify issues and service trends. Any survey with an individual component less than a 6 rating becomes an Improvement Opportunity and the specific issue is addressed by an interdepartmental task force, led by the Director of Customer Satisfaction.

SECTION 4: QUALITY PLAN OBJECTIVES AND METHODOLOGY

4.1 Quality Control Plan Objectives

- Generate and maintain a consistent view of the performance measurement data
- Perform reviews of the timeliness and accuracy of performance data
- Maintain a pro-active communication with our customer regarding the performance of the services we provide
- Ensure OTS is in compliance with the Departments expectations and requirements through excellent performance driven by systematic measurement and pursuing continuous quality improvement

4.2 Quality Control Plan Methodology

- Document the information that is expected by the customer based on contract and the Departments approval of CenturyLink's implementation plan
- Assign the responsible ownership for each service expectation
- Determine monitoring methods that must be put in place to provide the details of each reporting requirement to the Department
- Develop a timetable of each customer's reporting needs along with associated Quality review timeframes
- Maintain all Department required reporting on the CenturyLink Team secure customer portal (S-GATE)
- Schedule quarterly Department reviews to present trends in performance and to identify operational improvement opportunities

SECTION 5: QUALITY REVIEW PROCESS

5.1 Project Control Documentation Objectives

- The CenturyLink Team's staffing and resource plan, including equipment, telecom services, rates and appropriately meets the implementation schedule requested by our customer.
- Our Quality Control Plan appropriately represents the complexity and criticality of the customer's implementation requirements.

5.2 Installation Process Documentation

Daily updates to the Implementation Plan are required on all closed tasks and revision to the plan to address any open issues. Results of all measurements and metrics are documented and posted to a shared drive accessible to all the CenturyLink Team members. HEAT Tickets are used to document vital information that needs to be retained and accessible to the service team

5.3 Quality Control Inspections

CenturyLink's dedicated Project Manager will work with the Department's Project Manager to establish a process for conducting monthly Quality Control inspections which will help to ensure that offender telephones at each of the Departments facilities are maintained in good working order. These monthly inspections will be documented in the monthly maintenance reports for each facility. Our technicians will check each phone for physical damage a minimum of once a month and test the performance of all on site equipment at least once per month.

5.4 Monitoring Methods & Frequency

Our monitoring capabilities include a suite of diagnostic software that continuously monitors your hardware, software, and system performance from our Redundant Network Operation Centers in Atlanta and Dallas. This allows our personnel to diagnose and resolve issues on your system, often before you notice a problem yourself. Both commercial and proprietary technologies are used to gather system level status continuously from the call processing platforms.

Highly-trained technical support personnel continuously monitor facility servers connected to the OTS WAN (wide area network). Each call processing platform and supporting server or workstation is automatically polled every five minutes to determine its status. Graphical alarm indicators make it easy to see problem areas at a glance.

The monitoring system maintains an automatic and several-tiered alert notification system. Depending on different time thresholds and the severity of the problem, issues are automatically escalated to team personnel who are in a position to bring additional resources to bear to get those issues resolved quickly.

5.5 Call Detail Data Integrity and Monitoring

On a real time basis CDRs (Call Detail Records) are automatically recorded in our fully redundant data centers and copied to the billing production CDR Server and associated data bases. If CDR data is not being processed from a site for any reason, including legitimate

facility driven issues such as lock downs, the Network Operations Center recognizes this condition and opens a HEAT ticket for investigation.

The billing production group reviews all transmittals detailing daily call volume per facility and opens a trouble ticket to determine why a significant fluctuation occurred. All CDRs are stored in a centralized repository (CDR Data Base). This is an automated monitoring process that keeps track of the CDR files for all active sites. This repository also contains the different status of the CDRs and provides reports for billing operation monitoring.

Processes and procedures are in place to ensure the accuracy of all rates for calls originating from the Department's facilities. The Department specific rates will be uploaded to the Regulatory Drive and a Sales compliance Drive by the Governmental Affairs Department. A Billing Tables Specialist accesses this information to create the correct rate. Access to the rate tables is limited to the Billing Specialists and their Supervisor.

Any change to the rates must be initiated and approved by the Rates and Regulatory group. Signed approvals will be required at the Director level. All changes are documented by the HEAT Ticketing System. A Heat ticket is opened to initiate a rate table update on the platform. At the Technical Support Center our Technical Support Staff will review the rate sheets on the Regulatory shared drive or Sales compliance Drive to ensure when they load the new rate, that the rate matches the Rate Analyst approved rates. In addition, all rate table entries are reviewed by the Table Management Supervisor.

On daily basis, all billable calls are rated based on configuration tables. Within the rating process, there are control parameters that prevent duplication of CDR data. The rating process creates a "missing table configuration" report listing the site, error id and number of calls. This report is distributed to several Billing department personnel and managers. The table management group researches the report and resolves issues as quickly as possible. On a daily basis any CDRs identified on this report are re-processed through rating.

Once the CDRs are rated, files with unique layouts required by the LECs are created. These files are delivered daily to the LECs via password protected FTP. There is a defined control between the numbers of CDRs sent vs. the CDRs received. There are different methods on the confirmation itself, such as counts on header and trailers, transmittal reports and confirmation reports we receive from each of the LECs.

After the export CDR files are created, these are marked against the CDR data base repository, to track how many CDRs were received vs. how many were rated and exported. There are reports that detail how many CDRs were in the input, how many were in the output, and how many are missing processing (exception reports). These reports are reviewed on a daily basis and any back billing identified is processed by the billing analyst.

The billing production group keeps track of all files transmitted to the LECs. There is a daily log of all files that is kept and reconciled on a daily basis. At the end of the month it is also verified against the revenue reports generated. Number of CDRs and Rated amounts are matched between both reports to ensure all files and CDRs were included in the month end process.

ATTACHMENT H:
SAMPLE SCP
REPORTS

Secure Call Platform User Interface Sample Reports

SECURUS Technologies™

Secure Call Platform

connecting what matters

Authorized users enter username and password for anytime, anywhere access.

Log-In
Username

Password

[Forgot Your Password?](#)

Off The Wire
Securus Press Releases

Products & Services
Automated Information Services
Securus Video Visitation
Prepaid Calling Cards - Vending Machines
Inmate Debit Account
Secure Instant Mail

[Click Here To Access Facility Portal](#)

Selected Sample SCP Reports

- Call Detail Search Screen
- Call Detail Results Screen
- Three Way Call Detection Report
- Call Frequency Report
- Custody Account Call Usage Report
- Call Tracker Report
- Hourly Usage
- Covert Alert Report
- Officer Check In Report
- PAN Frequency and Detail Report
- PAN Management Report
- SCP Debit Report
- Voice Biometric Status Report
- Voice Biometrics Frequency of Failure Report
- Crime Tip Report
- Informant Line Report
- Emergency Call Report
- Word Spotting Search Report
- Comprehensive System Change Log
- Management Change Log
- Custody Account Change Log
- PAN Entry Change Log
- Phone Number Change Log
- User Management Change Log
- Security Template Change Log
- System Access Report
- Recording Log
- Scan Patrol Log

Sample Call Detail Search Criteria Screen

Call Detail Report (CDR) – Provides users with an intuitive and user friendly report that enables them to view or search on virtually anything related to an inmate call. SCP's Call Detail Report provides industry-leading investigative, fraud prevention, and administrative capabilities to all approved users from anytime, anywhere.

The screenshot displays the SECURUS Technologies interface for the Secure Call Platform. At the top, the user is logged in as ssullivan@SECUR.TX with a Facility Routing Number of 99001. The navigation menu includes HOME, SYSTEM, MONITOR, TOOLS, ADMIN, and FACILITY PORTAL. The main section is titled 'Call Detail Records Search' and features a 'FILL IN SEARCH CRITERIA' form. A callout box with blue arrows points to the search criteria fields, stating: 'Customize reports by changing search criteria--such as facility/site/phone/phone group, date range, call type, call termination, reason, call length, and much more.'

MANAGEMENT LEVEL

Facility	Site	Phone Group	Phone
Securus Demo Site	All Sites	All Phone Groups	All Phones

Call Detail Records Search Saved Searches

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches, and text areas with bold label allow multi-entries in comma separated.)

Country Code: Dialed Number: Destination Zone: -- ALL --

Custody Account #: PIN #: Prepaid Account #:

First Name: Last Name: Agency Type: -- ALL --

Termination Category: -- ALL -- Blocked Reason: -- ALL --

Call Type: -- ALL -- Call Status: Complete

Text2Connect: -- ALL --

Search Notes:

Tracker #: Call Tracker Notes: Note Type: -- ALL --

Alternate ID:

Inmate Grouping:

Date Criteria: Date/Time Range Results Per Page: 100

Start: 06/02/2016 00:00:00 End: 06/02/2016 23:59:59

Buttons: Search, Save Criteria, EXCEL, PDF, CSV, Reset

Sample Call Detail Results Screen

Call Detail Result Screen – After criteria have been selected and a user selects the “search” button, CDR results are shown. From these results, users can select a record, playback recorded calls, add a note, access audit logs for the record(s), save the record(s) to another medium, and much more.

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Facility: Securus Demo Site Site: All Sites Phone Group: All Phone Groups Phone: All Phones

Call Detail Records Search Saved Searches

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

3 Results PAGE 1 OF 1

SITE	PORT LOC	DIALED #	GEO LOC	START	END	DUR	ACCT #/ PIN	PREPAID ACCT#	NAME	AGENCY TYPE	CALL TYPE	CALL STATUS	TERM CAT	BLOCKED REASON	CALL PROPERTIES
Securus Demo Site	LP 16	(1) 9722770571 Local		06-02-2016 04:23:29	06-02-2016 04:25:12	103 (s) 1.72 (m)	998877 998877	424354359534	JENN TEST		Prepaid Calling Card	complete	Called party hangup		Language: English
Securus Demo Site	LP 16	(1) 9722770571 Local		06-02-2016 05:59:59	06-02-2016 06:00:36	37 (s) 0.62 (m)	998877 998877		JENN TEST		Debit	complete	Called party hangup		Language: English Charge: \$3.6 Taxes & Fees: \$0.46
Securus Demo Site	Princeton v2	(1) 800990011006		06-02-2016 11:23:22	06-02-2016 11:23:31	9 (s) 0.15 (m)	998899 225566		ALAN EDWIN		Visit Call	complete	Called party hangup		

EXCEL PDF CSV

Save selected calls to folder Add Selected to WS Queue

After search criteria have been selected, users can list to the recorded call, extend the expiration, download the recording, add a note to the record, select for scanning, save searches, or download to many different formats.

The functionality of SCP's Call Detail Report puts complete reporting capabilities for all calls at the fingertips of the user.

Three-Way Call Report

Three-Way Call Report – Investigators can run a comprehensive three-way report to display calls that have been flagged as having three-way activity. They can also use additional features to understand what happened to the call, make notes on the call, (and much more) – to uncover why the inmate attempted to “hide” the number. SCP can then be used to correct the behavior or flag the inmate or dialed number for further investigation.

The screenshot displays the SECURUS Secure Call Platform interface. At the top, the logo 'SECURUS Technologies' and 'Secure Call Platform' are visible. A navigation menu includes 'HOME', 'SYSTEM', 'MONITOR', 'TOOLS', 'ADMIN', and 'FACILITY PORTAL'. A 'Customizable search engine' callout points to the search interface.

The search interface is titled 'Call Detail Records Search' and includes a 'FILL IN SEARCH CRITERIA' section. A '3-way search criteria' callout points to the '3-way' checkbox, which is checked. Other search criteria include Country Code, Custody Account #, First Name, Last Name, Termination Category, Call Type, Text2Connect, Search Notes, Tracker #, Alternate ID, and Inmate Grouping. A 'Call is flagged as 3-way in SCP' callout points to the '3-way' checkbox.

At the bottom, a table shows search results. A callout 'Apply a number of different actions to the call' points to the 'Actions' column. The table has columns for Site, Phone, Dialed #, Date, Time, Duration, Agency, Call Type, Call Status, Term Cat, Block Reason, and Call Properties. The first result is for a call to '9728248294' on '06-13-2016 02:08:48' with a duration of '32 (s) 0.53 (m)'. The 'Call Properties' column shows 'Language: English', '3-Way', 'Voice Biometrics', 'CW Charge: \$3.6', and 'Taxes & Fees: \$0.46'.

Site	Phone	Dialed #	Date	Time	Duration	Agency	Call Type	Call Status	Term Cat	Block Reason	Call Properties
Securus Demo Site	PH 15300	(1) 9728248294 Local	06-13-2016	02:08:48	32 (s) 0.53 (m)	7899	Debit	complete	Caller Hang up		Language: English 3-Way Voice Biometrics CW Charge: \$3.6 Taxes & Fees: \$0.46

Sample Call Frequency Report

Call Frequency Report – an essential investigative report. The report allows users to look up phone numbers in the system that have been called a certain number of times, within a given time frame by using criteria, such as threshold (of the number of times a number was called), international, watched, private, termination category, call type, call status, and date range.

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Facility	Site	Phone Group	Phone
Securus Demo Site	>> All Sites	>> All Phone Groups	>> All Phones

Enter a threshold for the number of times a number was called to initiate the report. Select date range and other criteria to narrow the results.

Call Frequency Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches)

Threshold: *
Termination Category:
Call Status:
Call Type:
Start: *
End: *
International:
Watched:
Private:

Search EXCEL PDF CSV Reset

45 Results

PAGE 1 OF 5 > >>

EXCEL PDF CSV

SITE	DIALED #	FREQUENCY
Securus Demo Site	(1) 9728248294	30
Securus Demo Site	(1) 9729806830	24
Securus Demo Site	(1) 9722770608	23
Securus Demo Site	(1) 9729809807	22
Securus Demo Site	(1) 9722770571	18
Securus Demo Site	(1) 9722770547	17
Securus Demo Site	(1) 9722770600	15
Securus Demo Site	(1) 4692120328	14
Production Support	(1) 2149095672	12
Securus Demo Site	(1) 2149095672	11

Call Frequency results display each dialed number meeting or exceeding the defined threshold. By clicking on a frequency amount, all call detail information for the calls are displayed.

Sample Custody Account Call Usage Report

Custody Account Call Usage Report – allows users to view how much time an inmate spends on the phone for a selected period and whether or not they speak to the called party—right from an inmate’s Custody Account record. If required, full call detail reports are also available by entering an inmate’s name, PIN, or custody account number in the Call Detail Report.

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL
 Facility: Securus Demo Site >> Site: Securus Demo Site >> Phone Group: All Phone Groups >> Phone: All Phones

Custody Accounts
 Return to Account List

GENERAL ACCOUNT INFORMATION (* Indicates Required Fields)

Account #: 24680	Gender:	Activation Date:	Suspended: NO	Call Schedule: None Selected
Name: Chuong Test	Race:	Booking Date:	Start Date: N/A	3-Way Detect: DEFAULT
DOB:	Language Pref.: NONE	Date Last Released in SCP:	End Date: N/A	Max Call Dur: 2 minutes
SSN:	Housing Unit:	Alert Level:	Word Spotting: YES	
First Calls Free: NO	Virtual Group: None Selected	Agency Type: AKDOC	RCFD Action: ---	
Alternate ID	Inmate Grouping			
Alt-ID-02:	Alt-Grp-01:			

Misc Notes Voice Biometrics **Calling Usage** Debit Investigator Pro™

CALLING USAGE SEARCH
 Start: 05/30/2016 00:00:00 End: 06/27/2016 23:59:59
 Search Reset

CALLING USAGE REPORT
 *Private calls are included in usage, but may not be included with calling restrictions.

						USAGE (PER CALL TYPE)	
	ATTEMPTED	CONNECTED	ACCEPTED	DENIED	BLOCKED	SECONDS	MINUTES
DEBIT/TRUST FUND (Non-Private)	3	2	1	0	0	129	2.15
COLLECT (Non-Private)	16	6	0	1	1	0	0.0
FREE (Non-Private)	1	1	0	0	0	0	0.0
COMMISSARY IVR (Non-Private)	2	1	0	0	0	4	0.07
INSTANT PAY/FCC2 (Non-Private)	1	1	0	0	0	4	0.07
Total Calls (per Call Type)	23	11	1	1	1		
Total Accepted Calls (All): 1			Total Usage(All): 137 (Sec.) / 2.29 (Min.)				
Total Accepted Calls (Excluding Private Calls): 1			Total Usage (Excluding Private Calls): 137 (Sec.) / 2.29 (Min.)				

Sample Call Tracker Report

Call Tracker Report – an investigative report that allows users to track CDR notes (notes made by themselves or other investigators for a specific inmate call). Users can also export the report results to Excel, PDF, and CSV file formats.

SECURUS Technologies

ssullivan@SECUR.TX | Help | Log Out

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Facility	Site	Phone Group	Phone
Securus Demo Site	Securus Demo Site	All Phone Groups	All Phones

Call Tracker Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches)

Not Shared:

Tracking #: First Name: Last Name:

Custody Account #: PIN #: Dialed Number:




Notes:

Start Date/Time: 04/20/2016 00:00:00 End Date/Time: 05/17/2016 23:59:59

Results Per Page: 10

Search EXCEL PDF CSV Reset

1 Results PAGE 1 OF 1

CDR	TRACKING #	TRACKER NAME	DIALED #	ACCT#/PIN	NOTE
  		James LeBoeuf	9722770569	2008 2008	admitted guilt at 5:45

EXCEL PDF CSV

Search criteria for Call Tracker includes tracking number, first and last name, "not shared" (when checked), PIN, dialed number, keywords within the notes, and date range. Resulting report displays notes and other critical information about the call. In a single click, users can listen to the call, review full notations, and review full CDR information for the call.

Sample Hourly Usage Report

Hourly Usage Report – is a valuable administrative report that displays the number of phone calls that have taken place on a given date within a specific time range. Search criteria includes international, watched, private, call status, and date/time.

SECURUS Technologies

ssullivan@SECUR.TX | Help | Log Out

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Facility	Site	Phone Group	Phone
Securus Demo Site	Securus Demo Site	All Phone Groups	All Phones

Hourly Usage Report

FILL IN SEARCH CRITERIA (* Indicates Required Fields)
 (Use * for wild card / partial searches)

Call Status: Complete

Date Criteria: Date/Time Range (Note: Date Range Search Criteria is restricted to 1 week)

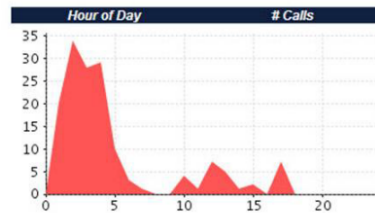
Start: 06/22/2016 00:00:00 End: 06/25/2016 23:59:59

International: Watched: Private:

Search PDF Reset

Results

PDF



Hour of Day	# Calls
00:00	0
01:00	20
02:00	34
03:00	28
04:00	29
05:00	10
06:00	3
07:00	1
08:00	0
09:00	0
10:00	4
11:00	1
12:00	7
13:00	6
14:00	1
15:00	2
16:00	0
17:00	7
18:00	0

Sample Covert Alert CDR Report

SCP's Cover Alert Feature – is a sophisticated investigative tool providing a live, call-forwarding feature for dialed numbers, phones, or PINs that are under surveillance by an investigative unit. This feature enables authorized personnel to monitor a call—undetected—from any designated location while the call is in progress and even “barge into” the call if necessary. **Covert Alert Report**—shows investigators the triggered Covert Alerts by useful criteria such as date/time, PIN, Alertee name/number, inmate name, dialed number, call status, and termination category. Reports can be exported into Excel, PDV, and CSV formats.

SECURUS Technologies

ssullivan@SECUR.TX | Help | Log Out

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Facility: Securus Demo Site Site: All Sites Phone Group: All Phone Groups Phone: All Phones

Covert Alert Call Detail Records Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches)

Alertee Country Code: Alertee Dialed Number: Alertee First Name: Alertee Last Name:

Country Code: Dialed Number: Custody Account #: PIN #:

First Name: Last Name:

Termination Category: -- ALL -- Call Status: -- ALL --

Date Criteria: Date/Time Range Start: 06/13/2016 00:00:00 End: 06/27/2016 23:59:59

Search EXCEL PDF CSV Reset

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.

100 Results PAGE 1 OF 10

SITE	PORT LOC	ALERTEE DIALED #	ALERTEE NAME	TERM CAT	START	END	DUR (S)	DIALED #	ACCT #/PIN	NAME	CALL STATUS	PIN ACCEPT
Securus Demo Site	LP 7	9722770556	Steve McGarrett	No Investigator Acceptance	06-13-2016 00:06:05	06-13-2016 00:06:39	34	2144981174	991133 991133	jose Zamora	complete	
Securus Demo Site	LP 7	9722770547	helen huynh	No Investigator Acceptance	06-13-2016 00:06:13	06-13-2016 00:06:48	35	2144981174	991133 991133	jose Zamora	complete	
Securus Demo Site	LP 7	9722770556	Steve McGarrett	No Investigator Acceptance	06-13-2016 00:17:41	06-13-2016 00:18:16	35	2144981174	991133 991133	jose Zamora	complete	
Securus Demo Site	LP 7	9722770547	helen huynh	No Investigator Acceptance	06-13-2016 00:17:50	06-13-2016 00:18:24	34	2144981174	991133 991133	jose Zamora	complete	
Securus Demo Site	hh test 4	9722770547	helen huynh	Parent Call Ended	06-13-2016 00:19:18	06-13-2016 00:19:35	17	9728248294	7890 7890	Helen Huynh	complete	
Securus Demo Site	hh test 4	9722770547	helen huynh	Parent Call Ended	06-13-2016 00:24:22	06-13-2016 00:24:25	3	9728248294	7890 7890	Helen Huynh	complete	
Securus Demo Site	hh test 4	9722770547	helen huynh	No Investigator Acceptance	06-13-2016 00:33:08	06-13-2016 00:33:43	35	9728248294	7899 7899	Helen Huynh	complete	
Securus Demo Site	hh test 4	9728248294	Helen Huynh	Terminated through Covert Alert	06-13-2016 00:33:27	06-13-2016 00:33:43	16	9728248294	7899 7899	Helen Huynh	complete	✓

Sample Officer Check-In Report

Officer Check-In Report – is a valuable administrative report showing users when officers have “checked in” at different phones and provides the ability to select and list to an messages they have left.

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Facility: Securus Demo Site >> Site: All Sites >> Phone Group: All Phone Groups >> Phone: All Phones

Officer Check In Messages Results

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches)

Account#: PIN: Officer ID: User Name:

First Name: Last Name: Call Status: Complete

Results per page: 10

Start: 06/13/2016 00:00:00 * 31 End: 06/27/2016 23:59:59 * 31
Format: mm/dd/yyyy HH:mm:ss

2 Results PAGE 1 OF 1 EXCEL PDF CSV

	SITE	PHONE LOC	NAME	USERNAME	ACCOUNT # / PIN	OFFICER ID	DUR	CALL STATUS	MESSAGE
	Securus Demo Site	hh test 4	Helen Huynh	helenh@SECUR.TX	JA-99999 99999	OfficerHuynh-99999	35 (s) 0.58(m)	complete	06-13-2016 00:28:52
	Securus Demo Site	hh test 4	Helen Huynh	helenh@SECUR.TX	JA-99999 99999	OfficerHuynh-99999	41 (s) 0.68(m)	complete	06-13-2016 00:49:33

Listen to messages that officers may have left during rounds.

Sample Personal Allowed Number (PAN) Frequency Report

Personal Allowed Number (PAN) Frequency Report – allows investigators to research multiple occurrences of phone numbers among PAN lists. Users have the ability to enter threshold numbers to define search criteria. For example, a threshold of “3” will show phone numbers that appear in PAN lists more than three times.

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL
 Facility: Securus Demo Site Site: All Sites

PAN Frequency Search
 FILL IN SEARCH CRITERIA (* Indicates Required Fields)
 (Use * for wild card / partial searches)

Threshold: 3 *

Search EXCEL PDF CSV Reset

204 Results PAGE 1 OF 21 EXCEL PDF CSV

SITE	DIALED #	FREQUENCY
Securus Demo Site	(1) 9722770311	25 🔍
Securus Demo Site	(1) 9722770596	22 🔍

PAN Frequency Detail Search
 FILL IN SEARCH CRITERIA (* Indicates Required Fields)

Country Code: 1 Dialed Number: 9722770311 *

Search EXCEL PDF CSV Reset

25 Results PAGE 1 OF 3 EXCEL PDF CSV

SITE	DIALED #	NAME	PIN
Securus Demo Site	(1) 9722770311	Automation Hammer 1	080001 080001
Securus Demo Site	(1) 9722770311	Burns Ken	0379 0379
Securus Demo Site	(1) 9722770311	CovertAlert FN87011	AC87011 87011
Securus Demo Site	(1) 9722770311	FGHFH FGHFDHDF	9000 90003816
Securus Demo Site	(1) 9722770311	Huynh test Helen	787878 787878
Securus Demo Site	(1) 9722770311	Huynh Helen	989898

Investigators enter a number into the threshold criteria field to research how many times phone numbers appear among the PAN lists of their facility and site(s).

By selecting the magnifying glass next to the displayed frequency number, users can run a detail report. This report shows information about each inmate having the number on their PAN list.

Sample Personal Allowed Number (PAN) Management Report

PAN Management Report – interactive report providing a dashboard view of all PAN entries in the system. If a PAN entry is entered through the Inmate-Managed PAN System, it is indicated on this report. Users can select from more than 20 criteria to produce reports with multiple data points. All reports are exportable to Excel, CSV, and PDF.

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL
 Facility: Securus Demo Site Site: Securus Demo Site

PAN Management Report

FILL IN SEARCH CRITERIA
 (Use * for wild card / partial searches)

Account #: [] PIN #: []
 Dialed Number: [1] [] [] Speed Dial: []
 City Code/Phone
 First Name: [] Last Name: [] Class of Service: []
 Source: [] Status: ACTIVE Verified: []
 Modified Start: [] Modified End: [] Results Per Page: 100
 Format: mm/dd/yyyy
 Relationship: [] Description: []

Blocked: Reason: All
 Private:
 Watch:
 Record Calls:
 Passive Acceptance:
 Allow on Suspend:
 3-Way Call Detect:

Search EXCEL PDF CSV Reset

1378 Results PAGE 1 OF 14 >>> CSV

*Your report is over 1,000 rows and can only be exported using CSV.

NAME	ACCT # / PIN	DIALED #	PAN APPROVED	VISIBLE	BLOCKED REASON	COB	SPEED DIAL	RELATIONSHIP	DESCRIPTION	PAN PRIORITIES	LAST MODIFIED
PALMER AAMODT	058050 058050	(1) 555-65555	Y	<input type="checkbox"/>	Friend and family request			Attorney		Blocked	25-Sep-2015
PALMER AAMODT	058050 058050	(1) 2142823695	Y	<input type="checkbox"/>	Harass			Brother	Brother	Blocked Watched	23-May-2014
PALMER AAMODT	058050 058050	(1) 2142823796	Y	<input checked="" type="checkbox"/>				Mother			07-Nov-2012
BRIAN AARESTAD	106954 1069546994	(1) 2144211213	Y	<input checked="" type="checkbox"/>					test		10-Nov-2010
BRIAN AARESTAD	106954 1069546994	(1) 2144219999	Y	<input checked="" type="checkbox"/>		Probono			214421		10-Nov-2010
BRIAN AARESTAD	106954 1069546994	(1) 9407658758	Y	<input checked="" type="checkbox"/>					AutoPAN 12		01-Jun-2016
BRIAN AARESTAD	106954 1069546994	(1) 9722140258	Y	<input checked="" type="checkbox"/>					tegr		10-Nov-2010
BRIAN AARESTAD	106954 1069546994	(1) 2144217777	Y	<input checked="" type="checkbox"/>		Operator: 22			214421		10-Nov-2010

Update Reset

PAN search criteria

Complete PAN detail with interactive

Sample SCP Debit Report

SCP Debit Report – is a valuable administrative report allowing users to:

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

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Facility: Securus Demo Site Site: Securus Demo Site Phone Group: All Phone Groups Phone: All Phones

SCP Debit Transaction Search
(Negative numbers will be displayed in parenthesis)

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches)

Inmate First Name: [] Last Name: [] Custody Account #: [] PIN: []

User Name: [] User Comments: [] Description: []

Type: --ALL-- Amount: --ALL-- Exclude Automated Process:

Note: Please limit search range to no more than 31 days

Start: 06/01/2016 00:00:00 End: 06/30/2016 23:59:59

Search Reset

By using the criteria in the search area, users can run reports detailing and totaling debit activity and balances for their facility

Site	Account # / PIN	Inmate First/Last	Type	Amount	Date/Time (In Central Time)	User	Reference #	Description	Comment
Securus Demo Site	0078 / 0078	KEVIN DORTINO	Credit	\$100.00	06/12/2016 10:40:30	kevinm@SECURUS.T	2016201210200-0078	Site Issued Credit	test money for deployment testing
Securus Demo Site	9888 / 9888	HELEN HUYNH	Credit	\$25.00	06/12/2016 09:45:36	helenh@SECURUS.T	20164512094535-9888	Site Issued Credit	
Securus Demo Site	7897 / 7897	HELEN HUYNH	Credit	\$25.00	06/12/2016 01:27:37	helenh@SECURUS.T	20162712012736-7897	Site Issued Credit	test account
Securus Demo Site	7899 / 7899	HELEN HUYNH	Credit	\$25.00	06/12/2016 01:24:45	helenh@SECURUS.T	20162412012444-7899	Site Issued Credit	

TOTALS

Action Type	Quantity	Amount
Payment	0	\$0.00
Credit	13	\$485.27
Debit	2	(\$55.05)
	15	\$430.22

Sample Voice Biometrics Status Report

Voice Biometrics Status Report – allows users to see the status and configuration settings for each site, custody account, phone number, phone group, and phone. This report also shows changes to an inmate’s account to assist administrators and investigators in tracking user accountability.

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL
 Facility: Securus Demo Site Site: Securus Demo Site Phone Group: All Phone Groups Phone: All Phones

Voice Biometrics Configuration Status Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)
 (Use * for wild card / partial searches)

Configuration Level: *
 Sites
 Custody Accounts
 Phone Numbers
 Phone Groups

Status: *
 All
 Enabled
 Disabled

Enrollment: *
 Enrolled
 Not Enrolled

Search Reset

55 Results PAGE 1 OF 6 EXCEL PDF CSV

INMATE NAME	CUSTODY ACCOUNT	ENROLLED	DEFAULT	ENABLED	DISABLED	SITE	ENROLLMENT LAST UPDATE BY	ENROLLMENT LAST UPDATE DATE
Chuong Test	24680	✓		✓		Securus Demo Site	Enrollment System	11-30-2011
Chuong Test	24680	✓		✓		Securus Demo Site	Enrollment System	01-20-2015
Francisco Burrows	9993	✓	✓			Securus Demo Site	Enrollment System	05-20-2015
Francisco Burrows	9993	✓	✓			Securus Demo Site	Enrollment System	05-20-2015
Gary Shipley	JEH8883	✓	✓			Securus Demo Site	Enrollment System	01-12-2015
Gary Shipley	JEH8883	✓	✓			Securus Demo Site	Enrollment System	01-12-2015
Helen Huynh	787878	✓		✓		Securus Demo Site	Enrollment System	05-05-2014
Helen Huynh	7899	✓			✓	Securus Demo Site	Enrollment System	06-12-2016
Helen Huynh	7899	✓			✓	Securus Demo Site	Enrollment System	06-12-2016
Helen Huynh	7897	✓	✓			Securus Demo Site	Enrollment System	06-13-2016

Status and Configuration search

Status and Configuration results, such as if the feature is enabled or disabled for an inmate, and if the inmate is enrolled--with single-click edit abilities from the screen.

Sample Voice Biometrics Frequency of Failure Report

Sample Voice Biometrics Frequency of Failure Report – an administrative and investigative report that allows users to see which inmates have failed voice biometrics verification attempts. Users may also see what percentage of inmates are passing or failing. Search criteria includes key information such as custody account, first and last name, and date range.

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL
 Facility: Securus Demo Site Site: All Sites

Voice Biometrics Frequency of Failure Search
**This report is updated and populated nightly for faster retrieval purposes.
 This is a report for Inmate name verification utterances to show the Frequency of Failure when an Inmate attempts to verify their name when placing a phone call.

FILL IN SEARCH CRITERIA (* Indicates Required Fields)
 (Use * for wild card / partial searches)

Custody Account #: First Name: Last Name:
 Start: 09/05/2016 * End: 09/30/2016 *
Format: mm/dd/yyyy

Search Reset

246 Results PAGE 1 OF 25 EXCEL PDF

INMATE NAME	CUSTODY ACCOUNT#	LAST FAILED VERIFICATION	LAST SUCCESSFUL VERIFICATION	% OF FAILED VERIFICATION	% OF SUCCESSFUL VERIFICATION
BRIAN AARESTAD	106954		09-30-2016		100.0
AMANDA ABARE	ASO09JBN001497	09-05-2016	09-25-2016	32.43	67.57
DWAIN ADKINS	206507	09-21-2016		100.0	
DAVID ALLGOOD	397066	09-23-2016	09-21-2016	94.87	5.13
ASDF ASD	0200635209	09-30-2016	09-21-2016	84.13	15.87
Joshua Abbott	3086		09-18-2016		100.0
TestDialup Acct1	11111	09-30-2016		100.0	
TestDialup Acct5	55555	09-11-2016	09-28-2016	33.33	66.67
Eva Adam	9900181	09-09-2016	09-17-2016	26.67	73.33
Christopher Adams	789456789456		09-30-2016		100.0

Search criteria to define frequency of failure report results

Report results detailing dates and statistics for biometric failures and successes for each inmate

Sample Crime Tip Report

Crime Tip – is a critical feature that enables anonymous two-way communication between inmates and facility staff. For inmates, the feature provides a secure method for reporting information about criminal activity. For facilities, the feature provides a flexible, configurable solution for gathering critical evidence to support investigations and prevent crimes from taking place in the facility. The Crime Tip Report shows detailed results for all Crime Tip calls. Results can be narrowed by using intuitive search criteria. Users can select to listen to, extend, download, add notes to, or audit each call record to manage the safety and security of their facility.

SECURUS Technologies ssullivan@SECUR.TX | Help | Log Out

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL
 Facility: Securus Demo Site Site: All Sites

TIPS Search
 FILL IN SEARCH CRITERIA (* indicates Required Fields)
 (Use * for wild card / partial searches)

Mail Box ID: Call Type: -- ALL --
 Date Criteria: Date/Time Range Results Per Page: 10
 Start Date/Time: 01/28/00:00:00 End Date/Time: 04/28/23:59:59
 Search Reset

35 Results << < PAGE 4 OF 4 > >> EXCEL PDF CSV

	SITE	PORT LOC	REPLY MAILBOX ID	CALL TYPE	START	END	DUR (s)
	Securus Demo Site	je test 4		Offender	04-19- 16:46:36	04-19- 16:47:01	0
	Securus Demo Site	je test 4		Offender	04-19- 16:49:39	04-19- 16:50:33	54
	Securus Demo Site	je test 4		Offender	04-21- 01:45:50	04-21- 01:46:42	52
	Securus Demo Site	je test 4		Offender	04-21- 01:51:03	04-21- 01:52:00	57
	Securus Demo Site	je test 4		Offender	04-21- 01:53:34	04-21- 01:54:03	29

EXCEL PDF CSV

Media player controls:

Sample Informant Line Report

SCP's Informant Line – is an investigative tool that allows inmates to communicate directly and anonymously with investigators. The call can be routed to a specific investigator, voicemail box, or answering machine. The Informant Line Report allows investigators to research and view details about these calls.

SECURUS Technologies | ssullivan@SECUR.TX | Help | Log Out

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Facility	Site	Phone Group	Phone
Securus Demo Site	All Sites	All Phone Groups	All Phones

Informant Line Call Records Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches)

Country Code: Dialed Number: Destination Zone: -- ALL --
Custody Account #: PIN #: Prepaid Account #:
First Name: Last Name:
Termination Category: -- ALL -- Call Status: Complete
Date Criteria: Date/Time Range Results Per Page: 100
Start Date/Time: 04/21/2011 00:00:00 End Date/Time: 04/28/2011 23:59:59
International: Watched:
Private: 3-way:
Voice Biometrics: RCF:

Search Reset

2 Results PAGE 1 OF 1

	SITE	PORT LOC	DIALED #	START	END	DUR	ACCT # PIN	PREPAID ACCT#	NAME	CALL STATUS	TERM CAT	CALL PROPERTIES
	Securus Demo Site	LP 17	{1} UNLISTED Local	04-21-2011 02:04:40	04-21-2011 02:04:59	19 (s) 0.32 (m)				complete	Called party hangup	
	Securus Demo Site	LP 17	{1} 9722770529 Local	04-21-2011 02:17:50	04-21-2011 02:18:02	12 (s) 0.2 (m)	00343			complete	Called party hangup	

Informant Line search criteria

Informant Line details and available actions.

Sample Emergency Call Report

SCP's Emergency Call – is an optional SCP feature allowing individuals to enter a bypass code to connect to facility personnel for emergencies, such a medical, violent, riotous, or suspicious incidents. For users who are authorized to view and listen to historical Emergency Calls, SCP provides an Emergency Call Report as shown in the image below.

SECURUS Technologies ssullivan@SECUR.TX | Help | Log Out

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Facility: Securus Demo Site | Site: All Sites | Phone Group: All Phone Groups | Phone: All Phones

Emergency Call Detail Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches)

ByPass Code: | Dialed Number: | Custody Account #: | PIN #:

Termination Category: -- ALL -- | Call Status: Complete | Results Per Page: 100

Date Criteria: Date/Time Range | Start Date/Time: 07/11/2016 00:00:00 | End Date/Time: 10/11/2016 23:59:59

Search Reset

1 Results PAGE 1 OF 1 EXCEL PDF CSV

	SITE	PORT LOC	BYPASS CODE	DIALED #	EXT. #	ACCT #/ PIN	START	END	DUR	CALL STATUS	TERM CAT	CALL TYPE	CALL PROPERTIES
	Securus Demo Site	Princeton 4	433	(1) 9722770433 Local			09-12-2016 16:50:01	09-12-2016 16:50:17	16 (s) 0.27 (m)	complete	Called party hangup	Emergency Call	

Save selected calls to folder

Emergency Call search criteria

Emergency Call details and available actions.

Sample Word Spotting Search Report

Word Spotting Search Report – is an essential investigative report that allows investigators to display all of the recordings that were submitted for Word Spotting processing with select criteria. Because Word Spotting is fully integrated with SCP, this report can be generated from the SCP user interface.

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Facility	Site	Phone Group	Phone
Securus Demo Site	All Sites	All Phone Groups	All Phones

Word Spotting Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

Country Code: Dialed Number: Key Word:

Custody Account #: PIN #:

First Name: Last Name:

Results per page: 10

Start: 04/25/2011 00:00:00 End: 04/27/2011 23:59:59

Search Reset

Enter criteria to narrow the search. Users can even search by the suspected key word flagged within the call.

Selected For Spotting:

- Lakers Tickets*
- Securus*
- Bullet*
- Heifer*
- Inmate*
- Weed*

Words For Search:

Sheriff*

3 Results PAGE 1 OF 1

SITE	PROF LOC	CTRY CODE	DIALED #	REG. SUBMIT TIME	ACCT # PIN #	NAME	USER NAME	FLAGGED WORD #	FLAGGED WORD # START	FLAGGED WORD # END
Securus Demo Site	LP 1	1	9722770490	04-26-2011 15:22:29	7890	Helen Huynh	WordSpot	Busted	00:00:50,27	00:00:50,59
Securus Demo Site	LP 1	1	9722770490	04-26-2011 15:22:29	7890	Helen Huynh	WordSpot	Hit	00:00:25,48	00:00:25,61
Securus Demo Site	LP 1	1	9722770490	04-26-2011 15:22:29	7890	Helen Huynh	WordSpot	Shot	00:00:19,28	00:00:19,57

View details of the report (including flagged word and the point in the call the word was flagged), listen to the call, download the call, or export the call.

Note: "2 seconds" buffer added to the Flagged Words StartTime and EndTime while playing the Recording.



Sample Comprehensive System Log Search

Comprehensive System Log Search – can be used by administrators to monitor the changes that have been made to the system. Administrators can use search criteria—such as username, name, and date range—to narrow their search. The tool can also omit changes made to the system through automated processes to narrow search results to only changes made by personnel.

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Facility: Securus Demo Site >> Site: All Sites >> Phone Group: All Phone Groups >> Phone: All Phones

Latest Activity Report Log Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches)

Username: First Name: Last Name:

Start: 09/11/2016 00:00:00 * End: 10/11/2016 23:59:59 * Exclude Automated Process:

Search EXCEL PDF CSV Reset

Select search criteria and omit automated changes

4 Results PAGE 1 OF 1

RECORD TYPE	RECORD DETAIL	MODIFIED FIELD	BEFORE	AFTER	ACCESS/MOD TIME (CENTRAL TIME)	USERNAME
System Access					10/11/2016 17:06:45	zabbix@SECUR.TX
Custody Account	padma123	PIN	NONE	123123123 (Created)	10/05/2016 07:34:34	padma@SECUR.TX
PAN	9728585858	Blocked	NONE	Employee number	10/05/2016 04:34:27	padma@SECUR.TX
DTN	7023735590	Dialing COS	NONE	Free	10/05/2016 02:36:17	padma@SECUR.TX

Sample Management Level Change Log Report

Management Level Change Log Report – can be used by administrators to monitor the changes made to features at each of the management levels. Administrators can use search criteria—such as username, name, and date range—to narrow their search.

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Facility	Site	Phone Group	Phone
Securus Demo Site	All Sites	All Phone Groups	All Phones

Management Level Change Log Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches)

Username: First Name: Last Name:

Start: * End: *

Format: mm/dd/yyyy HH:mm:ss

Search Reset

16 Results PAGE 1 OF 2 EXCEL PDF CSV

MANAGEMENT LEVEL	NAME	MODIFIED FIELD	BEFORE	AFTER	MODIFIED TIME (CENTRAL TIME)	USERNAME
Site	Securus Demo Site	Call Schedule	100520116	NONE (Deleted)	10/05/2016 04:56:32	
Site	Securus Demo Site	Call Schedule	NONE	100520116 (Created)	10/05/2016 04:55:40	
Customer	All Sites	Calling Restrictions	1padma	NONE (Deleted)	10/05/2016 04:53:31	
Customer	All Sites	Calling Restrictions	NONE	1padma (Created)	10/05/2016 04:52:51	
Customer	All Sites	Calling Restrictions	NONE	testingpadma (Created)	10/05/2016 04:50:21	
Site	Securus Demo Site	3-Way Call Detection	DISABLED	ENABLED	10/04/2016 13:58:01	cdang@SECUR.TX
Site	Kellway Test Lab Allen	Call Schedule		Wednesdays (Modified)	09/28/2016 14:36:06	jrvivas@SECUR.TX
Site	Kellway Test Lab Allen	Call Schedule		Wednesdays (Modified)	09/28/2016 14:35:48	sodea@I003298.TX
Phone Group	BPA	Call Schedule	4.3test	101 training	09/28/2016 10:12:22	bcarrell@SECUR.TX
Phone Group	Main	Maximum Call Duration	0	15	09/28/2016 10:11:51	bcarrell@SECUR.TX

Sample Custody Account Change Log Report

Custody Account Change Log Report – can be used by administrators to monitor the electronic and manual changes to custody accounts. Administrators can use search criteria—such as PIN, username, name, and date range—to narrow their search.

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Facility: Securus Demo Site Site: All Sites

Custody Account Change Log Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use ~ for wildcard / partial searches)

Username: _____ First Name: _____ Last Name: _____
 Custody Account Number: _____ Inmate First Name: _____ Inmate Last Name: _____
 Alternate ID: _____
 Inmate Grouping: _____
 Start: 09/11/2016 00:00:00 End: 10/11/2016 23:59:59 Exclude Automated Process:

Search EXCEL PDF CSV Reset

79 Results

PAGE 1 OF 8

EXCEL PDF CSV

ACCT #	NAME	MODIFIED FIELD	BEFORE	AFTER	MODIFIED TIME (CENTRAL TIME)	USER NAME
JEH1001	Brenda Dodger	Suspended	YES	NONE	10/11/2016 17:37:30	jhiggs@SECUR.TX
JEH1001	Brenda Dodger	Suspended Start Date	2016-09-22 16:24:23	NONE	10/11/2016 17:37:30	jhiggs@SECUR.TX
padma123	padma test	PIN	NONE	123123123 (Created)	10/05/2016 07:34:34	padma@SECUR.TX
padma123	padma test	Account Number	NONE	padma123(Created)	10/05/2016 07:34:34	padma@SECUR.TX
20152016	padma test	PIN	NONE	20152016 (Created)	10/05/2016 05:36:13	padma@SECUR.TX
20152016	padma test	Account Number	NONE	20152016(Created)	10/05/2016 05:36:13	padma@SECUR.TX
2010	padma alla	RCFD Action	DEFAULT	MARK ONLY	10/05/2016 04:28:26	padma@SECUR.TX
2010	padma alla	SSN	See account for details	See account for details	10/05/2016 04:28:26	padma@SECUR.TX
10052016	padma test	RCFD Action	DEFAULT	MARK ONLY	10/05/2016 04:26:05	padma@SECUR.TX
10052016	padma test	Middle Name		update	10/05/2016 04:26:05	padma@SECUR.TX

Sample PAN Entry Change Log Report

PAN Entry Change Log Report – 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.

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Facility	Site	Phone Group	Phone
Securus Demo Site	All Sites	All Phone Groups	All Phones

PAN Entry Change Log Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches)

Username:	First Name:	Last Name:
Ctry Code:	Phone Number:	
Custody Account Number:	Inmate First Name:	Inmate Last Name:
Start: 09/11/2016 00:00:00	End: 10/11/2016 23:59:59	Exclude Automated Process: <input checked="" type="checkbox"/>

Search EXCEL PDF CSV Reset

34 Results PAGE 1 OF 4

DIALED #	ACCT #	NAME	MODIFIED FIELD	BEFORE	AFTER	MODIFIED TIME (CENTRAL TIME)	USERNAME
(1) 9728585858	2010	padma alla	Blocked	NONE	Employee number	10/05/2016 04:34:27	padma@SECUR.TX
(1) 9728585858	2010	padma alla	Dialed Number	NONE	9728585858 (Created)	10/05/2016 04:34:27	padma@SECUR.TX
(1) 9722770601	10052016	padma test	Call Schedule	NONE	24/7	10/05/2016 03:40:22	padma@SECUR.TX
(1) 9722770601	10052016	padma test	3-Way Call Detection	DEFAULT	DISABLED	10/05/2016 03:40:22	padma@SECUR.TX
(1) 9722770601	10052016	padma test	Dialing COS	NONE	Free	10/05/2016 03:40:22	padma@SECUR.TX
(1) 9722770601	10052016	padma test	Dialed Number	NONE	9722770601 (Created)	10/05/2016 03:40:21	padma@SECUR.TX
(1) 9722770547	2012	Padma Alla	3-Way Call Detection	DEFAULT	DISABLED	10/05/2016 03:14:58	padma@SECUR.TX
(1) 9722770547	2012	Padma Alla	Dialing COS	NONE	Collect	10/05/2016 03:14:58	padma@SECUR.TX
(1) 9722770547	2012	Padma Alla	Dialed Number	NONE	9722770547 (Created)	10/05/2016 03:14:57	padma@SECUR.TX
(1) 9722770591	2010	padma alla	Call Schedule	NONE	24/7	10/05/2016 03:05:22	padma@SECUR.TX

Sample Phone Number Change Log Report

Phone Number Change Log Report – allows administrators to review all changes to controlled numbers on the Global list at both the agency and facility levels.

Secure Call Platform

Facility Routing Number: **99001**

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Facility	Site	Phone Group
Securus Demo Site	All Sites	All Phone Groups

Global List Change Log Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches)

Username:	First Name:	Last Name:
Ctry Code:	Phone Number:	
Start: 10/01/2016 00:00:00	End: 10/11/2016 23:59:59	Exclude Automated Process: <input checked="" type="checkbox"/>

1 Results

PAGE 1 OF 1

[EXCEL](#) [PDF](#) [CSV](#)

DIALED #	MODIFIED FIELD	BEFORE	AFTER	MODIFIED TIME (CENTRAL TIME)	USERNAME
(1) 7023735590	Dialing COS	NONE	Free	10/05/2016 02:36:17	padma@SECUR.TX

Sample User Management Change Log Report

User Management Change Log Report – allows administrators to review changes made to the account by selected users.

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Facility
Securus Demo Site

User Mgmt Change Log Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches)

MODIFIED: Username: First Name: Last Name:
 MODIFIER: Username: First Name: Last Name:
 Start: 10/01/2016 00:00:00 * End: 10/11/2016 23:59:59 *
Format: mm/dd/yyyy HH:mm:ss

Search Reset

69678 Results

PAGE 1 OF 6968 > >>

CSV

*Your report is over 5,000 rows and can only be exported using CSV.

SCP USERNAME	SCP NAME	MODIFIED FIELD	BEFORE	AFTER	MODIFIED TIME (CENTRAL TIME)	USERNAME
qwilliams@SECUR.TX	Quamesha Williams	PASSWORD		PASSWORD CHANGED	10/11/2016 16:16:48	qwilliams@SECUR.TX
ctruong@SECUR.TX	Cecilia Truong	PASSWORD		PASSWORD CHANGED	10/11/2016 16:03:19	ctruong@SECUR.TX
jgrayeskue@SECUR.TX	Jerry GrayEskue	CUSTOMER	NONE	Pennington County Juvenile, SD	10/11/2016 15:50:06	pmcguire@SECUR.TX
qwilliams@SECUR.TX	Quamesha Williams	PASSWORD		PASSWORD CHANGED	10/11/2016 15:28:17	qwilliams@SECUR.TX
CErickson@SECUR.TX	Chris Erickson	CUSTOMER	NONE	Pennington County Juvenile, SD	10/11/2016 13:47:37	pmcguire@SECUR.TX
tbessent@SECUR.TX	Terry Bessent	CUSTOMER	NONE	Pennington County Juvenile, SD	10/11/2016 13:45:52	pmcguire@SECUR.TX
swolfe@SECUR.TX	Stephon Wolfe	CUSTOMER	NONE	Pennington County Juvenile, SD	10/11/2016 13:44:13	pmcguire@SECUR.TX
sjordan@SECUR.TX	Sameka Jordan	CUSTOMER	NONE	Pennington County Juvenile, SD	10/11/2016 13:43:01	pmcguire@SECUR.TX
rthompson1@SECUR.TX	Rick Thompson	CUSTOMER	NONE	Pennington County Juvenile, SD	10/11/2016 13:41:29	pmcguire@SECUR.TX
mogarcia@SECUR.TX	Monica Garcia	CUSTOMER	NONE	Pennington County Juvenile, SD	10/11/2016 13:40:11	pmcguire@SECUR.TX

Sample Security Template Change Log Report

Security Template Change Log Report – allows administrators to review modifications made to security templates. Users can narrow their search by using criteria such as username, name, phone number, and date range.

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL
 Facility
 Securus Demo Site

Security Template Change Log Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches)

Username: First Name: Last Name:
 Modify Template: Start: End:

Search Reset

29 Results

PAGE 1 OF 3

EXCEL PDF CSV

SECURITY TEMPLATE	TYPE	MODIFIED FIELD	BEFORE	AFTER	MODIFIED TIME (CENTRAL TIME)	USERNAME
Tim Harris - restricted access	Modified	Monitor - View Live Calls	NONE	CAN VIEW	09/02/2016 12:47:58	tharris@I003298.TX
Tim Harris - restricted access	Modified	Monitor - View Live Calls	NONE	CAN EDIT	09/02/2016 12:47:58	tharris@I003298.TX
Tim Harris - restricted access	Modified	Monitor - Terminate Live Call	NONE	CAN VIEW	09/02/2016 12:47:58	tharris@I003298.TX
Tim Harris - restricted access	Modified	Monitor - Terminate Forwarded Call	NONE	CAN VIEW	09/02/2016 12:47:58	tharris@I003298.TX
Tim Harris - restricted access	Modified	Monitor - Terminate Forwarded Call	NONE	CAN EDIT	09/02/2016 12:47:58	tharris@I003298.TX
Tim Harris - restricted access	Modified	Monitor - Scan Patrol	NONE	CAN VIEW	09/02/2016 12:47:58	tharris@I003298.TX
Tim Harris - restricted access	Modified	Monitor - Listen to Live Calls and Recordings	NONE	CAN VIEW	09/02/2016 12:47:58	tharris@I003298.TX
Tim Harris - restricted access	Modified	Monitor - Forward Call	NONE	CAN VIEW	09/02/2016 12:47:58	tharris@I003298.TX
Tim Harris - restricted access	Modified	Monitor - Forward Call	NONE	CAN EDIT	09/02/2016 12:47:58	tharris@I003298.TX
Tim Harris - restricted access	Created				09/02/2016 12:46:17	tharris@I003298.TX

Sample System Access Log Report

System Access Log Report – allows administrators to manage user access by reporting lists of system users by date range. Users can narrow their search by using criteria such as username, name, and date range.

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL
 Facility
 Securus Demo Site

System Access Log Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches)

Username: First Name: Last Name:

Access Start: 09/11/2016 00:00:00 * Access End: 10/11/2016 23:59:59 *

Format: mm/dd/yyyy HH:mm:ss

26694 Results PAGE 1 OF 2670 [CSV](#)

**Your report is over 5,000 rows and can only be exported using CSV.*

USERNAME	NAME	TITLE	SECURITY TEMPLATE	IP ADDRESS	STATUS	LOG IN (CENTRAL TIME)	LOG OUT (CENTRAL TIME)	DURATION (MIN)
tsmith1@SECUR.TX	Taylor Smith		Securus Only-Cust Svc Rep I	209.163.225.158	Successful Login	10/11/2016 18:15:25		Unknown
khull@SECUR.TX	Kresha Hull		Securus Only-Cust Svc Rep III	209.163.225.158	Successful Login	10/11/2016 18:12:55		Unknown
ncofield@SECUR.TX	Nina Cofield		Securus Only-Cust Svc Rep I	209.163.225.158	Successful Login	10/11/2016 18:12:39		Unknown
zabbix@SECUR.TX	zabbix agent		Administrator	209.163.225.158	Successful Login	10/11/2016 18:11:44		Unknown
telmereyes@SECUR.TX	Esteban Reyes - TELM		Securus Only-TELM Employee	148.235.187.226	Successful Login	10/11/2016 18:11:02		Unknown
smckinnie@SECUR.TX	Shanice McKinnie		Securus Only-Cust Svc Rep I	209.163.225.158	Successful Login	10/11/2016 18:10:35		Unknown
jmorgan@SECUR.TX	Jamie Morgan		Securus Only-Cust Svc Rep II	209.163.225.158	Successful Login	10/11/2016 18:07:24		Unknown
zabbix@SECUR.TX	zabbix agent		Administrator	209.163.225.158	Successful Login	10/11/2016 18:06:44		Unknown
aechols@SECUR.TX	Adrian Echols		Securus Only-Cust Svc Rep I	209.163.225.158	Successful Login	10/11/2016 18:04:10		Unknown
amoton@SECUR.TX	Ariante Moton		Securus Only-Cust Svc Rep II	209.163.225.158	Successful Login	10/11/2016 18:02:34		Unknown

Sample Recording Audit Log Report

Recording Audit Log Report – allows administrators to report and manage all activity for recording usage. Administrators can search on key criteria such as recording usage, name, call start/end, access start/end, dialed number and PIN.

Secure Call Platform

Facility Routing Number: 99001

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Facility: Securus Demo Site >> Site: All Sites

Recording Audit Log Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches)

Username: First Name: Last Name:
 Recording Usage: -- ALL -- Dialed Number: Account #: PIN #:
 Call Start: End:
 Expiration Start: End:
 Access Start: 10/06/2016 00:00:00 End: 10/11/2016 23:59:59

Search Reset

3 Results PAGE 1 OF 1

ACCESS TIME	RECORDING USAGE	NAME	ACCT # / PIN	CALL START TIME	CALL END TIME	EXPIRATION DATE	USER	DIALED NUMBER
10-11-2016 17:43:18	PLAYBACK	BRENDA DODGER	JEH1001 101162	10-11-2016 17:40:36	10-11-2016 17:40:42	11/10/2016	jhiggs@SECUR.TX	9722770433
10-06-2016 15:23:10	SAVE TO FOLDER	GARY SHIPLEY	JEH8883 8883	07-05-2016 09:29:02	07-05-2016 09:29:23	11/02/2016	jgallo@SECUR.TX	2148830071
10-06-2016 15:20:45	PLAYBACK	GARY SHIPLEY	JEH8883 8883	07-05-2016 09:29:02	07-05-2016 09:29:23	11/02/2016	jgallo@SECUR.TX	2148830071

Media player controls: Play, Previous, Next, Stop, Pause, Fullscreen

Sample Scan Patrol Audit Log Report

Scan Patrol Audit Log Report – allows administrators to report and manage all activity for live monitor scans. Administrators can search on key criteria—such username and date range—to narrow their search. Users can also select to view the call detail records associated with each scan for additional information.

Secure Call Platform

Facility Routing Number: **99001**

HOME SYSTEM MONITOR TOOLS ADMIN FACILITY PORTAL

MANAGEMENT LEVEL

Facility: Securus Demo Site >> Site: All Sites

Scan Patrol Audit Log Search

FILL IN SEARCH CRITERIA (* Indicates Required Fields)

(Use * for wild card / partial searches)

Username:

Start: 07/15/2016 00:00:00 * End: 08/11/2016 23:59:59 *

Format: mm/dd/yyyy HH:mm:ss (CST)

2 Results **PAGE 1 OF 1** [EXCEL](#) [PDF](#) [CSV](#)

SITE	START	END	USERNAME
Securus Demo Site	07-28-2016 17:31:45	07-28-2016 17:32:32	jhiggs@SECUR.TX
Securus Demo Site	07-27-2016 17:55:11	Unknown	jhiggs@SECUR.TX