3.7.12 The security and confidentiality of data in the ITS is of critical importance. The vendor will recover all inmate telephone data for all locations, to the point of full service operation using a data backup.

The vendor will perform all service and database back-ups and archiving. The vendor will provide all archival hardware, supplies, and network recovery procedures to ensure no data is lost at no cost to the NDOC.

CenturyLink has read, understands and will comply.

All NDOC facilities will be connected to our San Antonio data center which is housed in a fire and flood-proof building with redundant fiber access, multiple power sources with a generator-powered UPS. The San Antonio data center will be backed up by our data center in Atlanta, where all NDOC data will be replicated.

3.8 DATA STORAGE

3.8.1 The vendor will perform all ITS database back-ups and archiving including all call records, ITS programming database and call recordings. All archival hardware, supplies, network and recovery procedures, which ensure no data will be lost, will be provided by the vendor at no cost to the NDOC.

3.8.1.1 The vendor will briefly describe how they will perform back-up or ITS redundancy of call data.

CenturyLink has read, understands and will comply.

CenturyLink will provide a completely centralized solution with all data sessions hosted and call records/recordings stored in our San Antonio data center. Copies of all call recordings and data will also be replicated to the CenturyLink data center in Atlanta for back up and disaster recovery purposes.

NDOC's facilities will be connected by an always-on, fully-managed, secure WAN to our San Antonio data center. This data center is housed in a climate-controlled, fire-proof, flood-proof building with unique redundant fiber lines to the national grid, multiple independent power sources and multi-level, multi-technology access control for unequaled security and database and network uptime. We will continue to provide online storage of all data and records with guaranteed instant access for the full term of the contract at no cost to NDOC.

3.8.2 The vendor will provide full ITS programming back-up on a daily basis including, but not limited to:

3.8.2.1 All call restrictions;
3.8.2.2 ITS inmate ID numbers;
3.8.2.3 Recorded inmate names;
3.8.2.4 ITS prompts; and
3.8.2.5 Other ITS operating database information.

CenturyLink has read, understands and will comply.

The data in subsections 3.8.2.1 through 3.8.2.5 will be continuously backed up in near real-time at our secondary data center in Atlanta.

3.8.3 The vendor will provide full ITS programming back-up in real time including, but not limited to:

3.8.3.1 All call restrictions;
3.8.3.2 ID;
3.8.3.3 Recorded inmate names;
3.8.3.4 ITS prompts; and
3.8.3.5 Other ITS operating database information.

For example, when an Administrator updates an inmate's ID, the ITS automatically backs-up such changes immediately to the vendor's off-site location.

CenturyLink has read, understands and will comply.

Please see our previous response to Subsection 3.8.2 immediately preceeding this subsection.

3.8.4 The vendor will provide full ITS inmate call record back-up from each NDOC location on a daily basis.

CenturyLink has read, understands and will comply.

With the centralized solution, all call data is replicated and backed up in real-time. Call data and recordings are sent over the network to the storage servers in our San Antonio data center. Call data and recordings are then replicated to a secondary CenturyLink data center in Atlanta.

3.8.5 The vendor will provide full ITS inmate call record back-up in real time. For example, when an inmate has completed all information regarding the call, the vendor will back-up immediately to the vendor's off-site location.

CenturyLink has read, understands and will comply.

Because we are offering a centralized solution, all inmate call records are replicated and backed up in real-time. Call data and recordings are created on the centralized platform and written in real-time to the storage servers at our current primary Data Center in San Antonio. Call data and recordings are then replicated to the CenturyLink data center in Atlanta. This backukp isdone throughout the day with minimal delay; the data will be replicated in Atlanta within seconds of the call being completed.

3.8.6 The vendor will provide full ITS inmate call recording back-up from each NDOC location on a daily basis.

CenturyLink has read, understands and will comply.

With our new centralized solution (discussed previously), no call data will reside at any NDOC facility; call data and call recordings are written in real-time to the database and storage servers

at our primary Data Center in San Antonio. Call data and recordings are then replicated to the secondary CenturyLink data center in Atlanta.

3.8.7 Vendor will provide full ITS inmate call recording back-up in real time. For example, when an inmate call completes, the entire recording of that call backs-up immediately to the vendor's off-site location.

CenturyLink has read, understands and will comply.

Because we are proposing a centralized architecture, all data will be hosted off-site at our dat center in San Antonio. There will be no local database at the facility to keep current. All data is maintainedoff-ste and will be backed up to our secondary data center in Atlanta

3.8.8 The vendor will briefly describe how the local ITS databases at all NDOC facilities will be kept current with the ITS back-ups at the vendor's off-site location in case of required re-programming or ITS recovery at the NDOC facility. Should the vendor permanently lose call data, vendor will be responsible to the NDOC for reimbursement.

CenturyLink has read, understands and will comply.

Because we are proposing a centralized architecture, all data will be hosted off-site at our data center in San Antonio. There will be no local database at the facility to keep current. All data is maintained off-site and will be backed up to ouir secondary data center in Atlanta..

3.8.9 The vendor must agree that the NDOC retains ownership of all archived information, call detail, inmate records, call recordings, etc. The vendor must agree that the NDOC has the right to obtain all achieved information, call detail, inmate records, call recordings, etc. associated with the ITS regardless of the location of such information within the vendor's organization or site.

CenturyLink has read, understands and will comply.

3.8.10 The ITS will store all call detail records, including all attempted and completed calls. This data will be stored at the vendor sites throughout the duration of the Contract. Upon successful ITS implementation, the vendor will either import the previous year's telephone data or pay the previous vendor to provide one (1) year of call record storage and retrieval at no cost to NDOC.

The vendor will provide authorized NDOC staff with a "Certificate of Destruction".

CenturyLink has read, understands and will comply.

As the incumbent vendor, CenturyLink has access to all recordings made over the last six years, and will import all telephone data from that timeframe from the existing system to the new centralized platform to allow NDOC access to that data. CenturyLink agrees to also keep all data on-line for the life of the contract, ensuring NDOC will have the ability to retrieve data as far back as 2006.

3.8.11 The ITS will record all data with a historical transaction record. All data will be stored/archived for retrieval/backup in a database when requested by authorized NDOC staff in accordance with the following:

3.8.11.1 All historical data will be centrally stored and accessible for reporting purposes.

3.8.11.2 This information must be available for reporting in a format of

3.8.11.3 The vendor is required to store telephone data throughout the duration of the Contract and/or successful transfer of the data to the authorized NDOC staff. Call records detail and call recordings will be available "on-line" for a minimum of twelve (12) months from the date of the call and call records detail will be available "off-line" for an additional forty-eight (48) months, or a total of sixty (60) months from the date of the call. "Off-line" records will be in a format readily accessible to the authorized NDOC staff upon request.

3.8.11.4 All data will remain the property of the NDOC and the vendor will not use the data for any purpose other than as required in the Contract.

CenturyLink has read, understands and will comply with Subsections 3.8.11.1 through 3.8.11.4.

With regards to the requirements in 3.8.11.3, as the incumbent vendor for NDOC, CenturyLink stores all data on-line; we do not store any data off-line. NDOC currently has immediate access to any data; this will continue to be our practice if CenturyLink is selected to continue to supply inmate telephone services to the State.

3.8.12 The vendor will have a written Disaster Recovery Plan and Continuity of Operations Plan and associated internal system equipment that will be capable of providing for support in case of failures in power, ITS data networking, and vendor's equipment at its host site through the user-level equipment provided by the vendor, and for all natural or man-made disasters including flood or fire at the host facility. These plans and all updates will be reviewed and accepted by the authorized NDOC staff and kept for reference purposes.

CenturyLink has read, understands and will comply.

The following Disaster Recovery Plan is similar to what is in place today on the existing inmate phone contract with modifications to address the transition to a state of the art centralized calling platform. CenturyLink will work closely with NDOC staff to review and modify this plan as needed upon contract award to ensure full compliance.

Disaster Recovery and Service Continuity
CenturyLink will provide a completely centralized solution with all data sessions hosted and records/recordings stored in our San Antonio, Texas data center. Copies of all call data will also be replicated to the Atlanta, Georgia data center for back up and disaster recovery purposes. Copies of all call detail records will be stored in two separate geographical locations.

Critical system data, call records and call recordings are stored on non-volatile hard disks in RAID arrays to ensure that any interruption in power does not result in loss of call records. The disk array provides both reliability and redundant drives for maximum protection of the facility's data.

Our data centers are housed in climate-controlled, fire-proof, flood-proof buildings with unique redundant fiber lines to the national grid, multiple independent power sources, and multi-level, multi-technology access control for unequaled security and database and network uptime. CenturyLink is prepared to respond quickly in the unlikely event that a true disaster occurs, completely destroying a primary or backup system.

Additionally, each system is monitored on a 24/7 basis utilizing the Nagios monitoring applications, which monitors both hardware and application software status. In the event of a failure, the application will generate alerts to the appropriate rapid response personnel.

Disaster Recovery Plan
CenturyLink's management team recognizes the importance of maintaining an effective Disaster Recovery Plan to help ensure the continuity of critical business processes and minimize disruption in the event of material disruption.

Our internal planning covers:

1. ***Disruption or disaster at a client facility***
2. ***Disruption or failure of a managed WAN or third-party network service (i.e., LIDB validation)***
3. ***Disruption or disaster at a CenturyLink data center***
4. ***Loss of key personnel***

Each separate plan identifies a primary and back-up Incident Commander (IC).

Type 1 – Onsite Equipment Disruption
Please note that the calling system is fully centralized, with most critical system components located offsite in redundant, geographically separate data centers. Onsite equipment is limited to just the phone instruments themselves, UPS backup power, and Integrated Access Devices (IADs) that connect the phones to the offsite call processors.

CenturyLink installs multiple IADs at each facility. In the event that one of our IADs fails, the inmate phones will be automatically routed to the next available IAD, without any interruption to inmate calling. While extremely remote, lin the event of a catastrophic failure of all IADs, all of our field service technicians maintain spare components and gateways and will be immediately dispatched to the facility to replace the defective IADs. In the event of an onsite disaster that damages most or all of the onsite equipment, the following procedure will be initiated.

For a Type 1 disaster the primary IC will be Debra Lambe (NDOCProgram Manager), with Barry Brinker (Director of Service Operations) as the back-up. Each will be closely acquainted with DOC staff and procedures. They will be alerted by our 24/7/365 Technical Services Center and will:

1. ***Immediately coordinate a visit from themselves or our local technician to assess the damage and put the Technical Support Team on notice.***
2. ***They will then determine the extent of the damage and the need for replacement parts, as well as the availability of space, and if needed, a network access point for communication***

services, and present a plan to the facility to restore all services.

3. *Technical Support team will ship the new system components*
4. *Ms. Lambe or Mr. Brinker will join a member of the Engineering team and our local technicians for onsite equipment installation, including new wiring as necessary.*

Type 2 – Network Connectivity Disruption

Please note that, for each supported facility, CenturyLink obtains network service from two different network carriers, (each network is sized to carry the full network load) so that if one carrier experiences an outage, service will instantly fail over to the second carrier. While the following plan will be initiated anytime a network service outage is detected, phone system access will continue to operate normally except in the highly unlikely event that a disaster should impede service of both network carriers simultaneously.

For a Type 2 disaster the primary IC is Joe Stables (Engineering/Network Manager) and the back-up is Chris Walton (Network Supervisor). Type 2 incidents may also require a full Crisis Response Team (CRT) drawn from the technical staff of our Network Operations (NetOps), Operations, Installation, Engineering and Management teams.

The IC will be notified by our network monitoring applications or a ticket opened online by facility staff or a call into our 24/7/365 Technical Services Center, or by one of our network or database providers and their monitoring staff. The IC will:

1. *Immediately notify the network provider and our Network Specialists and Engineering team leaders, who will begin diagnostics and re-route traffic*
2. *Determine based on the severity of the incident whether or not to form a full Crisis Response Team including CenturyLink' Management (if so, Joe Stables (Engineering/Network Manager) and Chris Walton (Network Supervisor) will take charge*
3. *Notify NDOC*
4. *Determine whether to involve CenturyLink Management*
5. *Present a plan to re-route all traffic and/or restore normal service*
6. *Make our Network carriers aware of SLAs and escalate as entitled under our service contracts*
7. *Coordinate operational response from our carriers and NetOps and Engineering teams to re-route traffic, restore normal service*
8. *Share progress and resolution with NDOC*

Third-party validation sources have built-in redundancy and have proven over the years to be reliable. Any risk of loss regarding third-party support is believed to be minimal since key vendors already have redundancy and failover mechanisms in place. Network common carriers and dial-tone providers maintain their own disaster recovery plans pursuant to applicable regulatory requirements, and CenturyLink' third-party services are also distributed among multiple vendors.

Any network outage should be diagnosed from our primary data center and Network Operations Center (NOC) in San Antonio. In the event of a third-party utility outage such as a cut power line, Mr. Stables, Mr. Walton, or the most available backup IC would coordinate directly with local utility.

Type 3 – Data Center Disruption

CenturyLink currently maintains two data centers. Our primary data center is located at our partner's headquarters in San Antonio, Texas. Our secondary data center is located 900 miles

away in Atlanta, Georgia.

Each office serves as a back-up site for the other. Source code for all applications supported from a location is spooled weekly to a server at the other location. Call data is transmitted instantly to both data centers, ensuring backup copies of all investigative data are always available. DOC facilities would experience a disruption to these services only in the very unlikely event that disasters should impact both data centers. Regardless, Type 3 incidents will be initiated as outlined below, anytime a service disruption is detected at either data center.

For a Type 3 incident Barry Brinker (Director of Service Operations) will be the primary IC, with Joe Stables (Engineering/Network Manager) as the secondary IC, if Mr. Brinker is not immediately available. A Type 3 incident will be detected immediately by CenturyLink's staff and system monitoring applications. For any Type 3 incident, a Crisis Response Team will be formed with Mr. Brinker or Stables coordinating Engineering and Operations teams at the remaining data center.

- *Core Technology: CenturyLink maintains nightly off-site backups of all source code and compiler tools to enable recreation of the support environment virtually anywhere within a few hours.*
- *All other systems such as reporting, accounting, etc. are backed up nightly and could be restored quickly onto "off-the-shelf" hardware. Our staff can build a new server stack from readily available hardware and install it at an unaffected co-location to restore redundancy in short order.*

In the event that a temporary replacement system must be set up at another data center (such as if a data center were completely destroyed in a natural disaster), CenturyLink has a nationwide procurement and inventory management system that can be used to quickly procure replacement equipment. An Engineering team can be mobilized to assemble, load, and test a server stack and related systems for installation in a near-by commercial facility, if a prolonged downtime at one of our data centers is expected.

CenturyLink' Engineering team is prepared and able to configure, ship, and replace any damaged or failed system within 12 to 24 hours from on-hand materials, depending on the number of facilities affected. The CenturyLink Team has installed over 200 centralized calling platforms, so our ability to do so reliably and under deadline is tested and validated regularly in the course of normal operations.

Type 4 – Loss of Key Personnel
Any company is vulnerable to the loss of key personnel, and CenturyLink' management is diligent in cross-training and knowledge transfer among our departments in order to minimize the disruption caused by the loss of a key individual. Specific personnel backup designations have been established to assist in contingency planning. Each key staff member has a backup.

All of CenturyLink' disaster response and business continuity plans are subject to an annual internal review by our Executive Management team, who have more than 60 years of experience managing the reliable provision of services to correctional agencies nationwide. Dry runs testing the ability of IC and secondary staff to identify and evaluate disruptions are held at least annually. The timely delivery of parts and supplies is tracked and measured constantly to be sure our supply chain is providing the parts needed to provide or restore service in a timely fashion for all of our clients. The performance of all network and network service providers is monitored constantly, and their adherence to SLAs, uptime, and reliability standards is measured and reported monthly.

3.9 SECURITY FEATURES

3.9.1 The ITS will allow multiple operators simultaneous access while maintaining adequate security to prevent unauthorized use and access.

CenturyLink has read, understands and will comply.

There is no practical limit on the number of operators that can have access to the System at one time Security ws discussed previously in Section 3.4.2 and below in Section 3.9.2.

3.9.2 The ITS will contain security features, which prevent unauthorized individuals from accessing any information held by the vendor. Secure access to the ITS and the database will be maintained at all times.

CenturyLink has read, understands and will comply.

Over the last six years, NDOC has used CenturyLink's Enforcer System, and is very familiar with our security features. A brief overview of the security features is provided for documentation.

Anyone desiring access to the System must be set up by a NDOC Site Administrator, who will set up the "role", which is, essentially, a generic job description for an Enforcer user—i.e., a person who performs certain functions for a correctional facility, for a law enforcement agency, or for an ICSolutions' business partner. When a new user is set up initially to use the ENFORCER, the Site Administrator can assign a user the permission to perform a defined group (list) of tasks. This group is assigned a meaningful role name, such as Intake (for an intake officer), or Site User (for Enforcer administrative personnel at a site).

To simplify setup of a user in the Enforcer, every new user must be assigned a role name.

The Enforcer Site Administrator: can

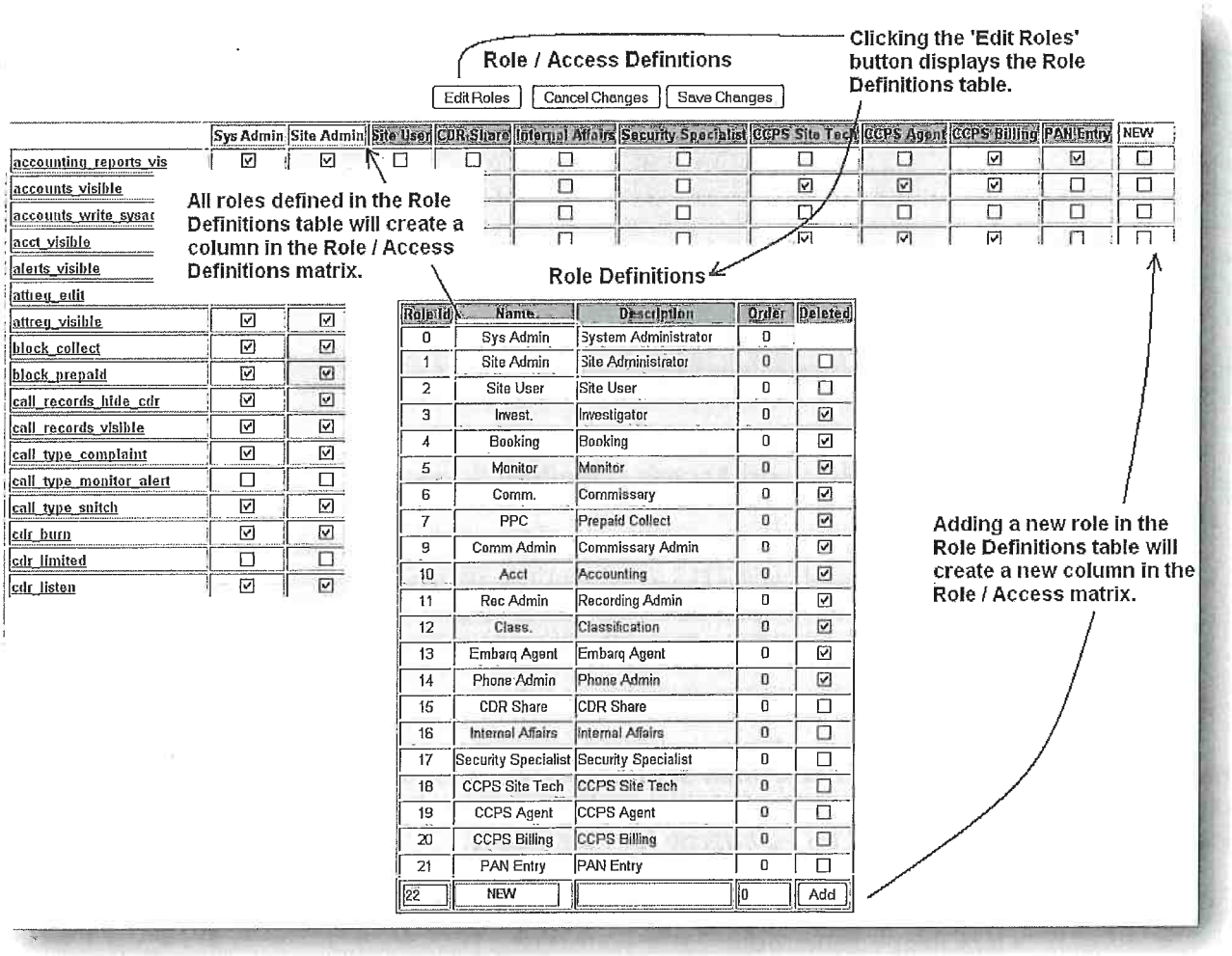
- ***Assign one or more role names to a user***
- ***Change the tasks currently assigned to a role name***
- ***Define a new role, and assign a group of tasks to it***
- ***Delete a role***

A standard list of roles is already in existence to correspond to the key job functions at NDOC; however, new roles can be added to the existing list, or roles can be deleted.

Enforcer Functions
Because of its diverse functionality, the System utilizes a matrix of function codes, each which grants specific user rights (functions) to the role. These rights may include any of the following:

- ***View-only access to certain information***
- ***Capability to change inmate profile information***
- ***Capability to view or make adjustments to inmate calling accounts***
- ***Access to call records, alerts, and recordings***
- ***Capability to perform certain tasks, such as copying call records to a CD***
- ***Capability to generate selected Enforcer reports***
- ***Access to optional Enforcer interfaces or tools***

After assigning a user to a role, the Site Administrator enables specific functions for the role. The screenshot below summarizes how the screens accessible under the Roles quick link can be used to quickly set up, change, or delete user rights for a role. "Functions" are the elements on the far left of the screen:



Role and Access Definitions Example

By selecting or deselecting check boxes in the Role/Access Definitions matrix shown on the following page, users are granted permission for that role (column heading) to perform the selected view/edit task (row).

Role / Access Definitions

Edit Roles | Cancel Changes | Save Changes

	Sys Admin	Site Admin	Site User	Invest	Booking	Monitor	PPC	Acct	Rep Admin	CDR Share	Cust Serv	HRInmate Share	CDR Limited
accounting_reports_vis	☑	☑	☐	☐	☐	☐	☐	☑	☐	☐	☑	☐	☐
accounts_visible	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐
accounts_write_sysadm	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
acct_visible	☑	☑	☐	☐	☐	☐	☑	☐	☐	☐	☑	☐	☐
alerts_visible	☑	☑	☑	☑	☐	☐	☐	☐	☑	☐	☐	☐	☐
attreg_edit	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
attreg_visible	☑	☑	☑	☑	☑	☑	☑	☐	☑	☐	☑	☐	☐
block_collect	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
block_prepaid	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
call_records_hide_cdr	☑	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐
call_records_visible	☑	☑	☑	☑	☐	☑	☑	☐	☑	☐	☑	☐	☐
call_type_complaint	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐
call_type_monitor_alert	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Role and Access Definition Screen

3.9.3 The vendor will establish an "informant" line. Calls to the "informant" line will be free and will be routed via the ITS to a destination designated by authorized NDOC staff. If so requested by authorized NDOC staff, the destination for the "informant" line may be an automated voicemail box. This call will not be a charge to the inmate.

CenturyLink has read, understands and will comply.

CenturyLink has implement informant lines at multiple facilities; this feature can be routed to various destinations including a voicemail box, an 800 number, or a local NDOC office number, among other options. There will be no charge for these calls.

3.9.4 The ITS provided by the vendor will not be capable of being detected by the called party for calling number identification (caller ID).

CenturyLink has read, understands and will comply.

The information that will be displayed on a caller ID will be determined by NDOC. This could be "Unknown Number" or the toll-free number for CenturyLink's customer call center, among other options. Currently NDOC has (702) 262-6140 displayed. This number is directed into the Inmate Voice Messaging System, and if called, allows the called party to leave an inmate a 30 second voice mail.

3.9.5 The ITS will prohibit direct-dialed calls of any type.

CenturyLink has read, understands and will comply.

All inmate calls must go through the Inmate Telephone System for authentication and validation. There is no possibility for the inmate to circumvent this process; direct-dialed calls are never allowed.

3.9.6 The ITS will prohibit access to "411" information service.

CenturyLink has read, understands and will comply.

As a standard feature of the System, calls to 411 and toll-free (800) numbers are blocked. However, at NDOC's discretion, an 800 number, for example to a PREA hot-line, can be unblocked.

3.9.7 The ITS will prohibit access to NDOC designated numbers.

CenturyLink has read, understands and will comply.

As the incumbent provider of inmate telephone services for NDOC, over the last six years CenturyLink has built, in conjunction with NDOC, a comprehensive list of designated numbers. If CenturyLink is awarded the new contract, NDOC and the new vendor will not need to implement a new process to develop a designated numbers list.

3.9.8 The ITS must be able to be shut down quickly and selectively. Authorized NDOC staff must be able to shut down the ITS by cut-off switches at several locations including, but not limited to:

3.9.8.1 At demarcation location - total facility telephones;
3.9.8.2 By central control center - select telephones; and
3.9.8.3 By select housing units - control center.

CenturyLink has read, understands and will comply.

In addition, the Enforcer is configured to support cut-off of the inmate phone system by individual phone other configurations if required by NDOC; this was discussed previously in Subsection 3.4.7.

3.9.9 The ITS will be able to take an individual telephone out of service without affecting other telephones.

CenturyLink has read, understands and will comply.

This is a standard feature of the System, and was discussed in greater detail in Subsection 3.4.7.

3.9.10 The ITS will not process incoming calls at any time. The vendor shall agree that no inmate telephone will be capable of receiving an incoming call and the vendor will work with the local exchange carriers (LECs) to ensure such control.

CenturyLink has read, understands and will comply

The design of the Enforcer routes a call from an NDOC facility to a processor which then distributes the call over the telephone network to the called party. There is no telephone number that exists for the Enforcer, and there is no direct connection with a LEC, thus there is no possibility that an incoming call can be completed. In the six years that CenturyLink has provided service to NDOC, there has never been an incoming call completed.

3.9.11 The vendor will describe how it detects "false disconnects".

CenturyLink has read, understands and will comply.

The ITS accurately detects valid forms of disconnect: inmate hang-up, called party hang-up, and forced hang-up (such as when reaching the call duration limit, or for a security violation). In the case of inmate or called party hang-up, the ITS receives a valid disconnect message from the network. In the case of a forced hang-up, the reason for the disconnection is noted in the Call Detail Record.

A dial tone is never provided to the inmate caller, either before or after a call. Therefore, attempts at "hookswitch flashing" are impossible. The ITS does not allow any way for the inmate to accomplish a "false disconnect" in order to establish a 3-way call, forward a call to another number, or otherwise obtain a secondary dial tone. Any such attempts are detected by the ITS and, in addition to being unsuccessful, are flagged in the CDR for investigation. Depending upon the NDOC's preferences, the detection of fraud attempts can also trigger the playing of a warning message to the inmate and called party and termination of the call that is in progress.

3.9.12 The ITS will have the capability of answer detection.

CenturyLink has read, understands and will comply.

The ITS uses answer detection to recognize busy signal, ring no answer, and invalid number announcements (SIT Tones). Upon detecting answer, the system will only acknowledge positive acceptance by the called party. Answering machines, pagers and voice mail responses will all be treated as incomplete calls. Only a positively accepted call will generate a call charge to the paying party.

3.9.13 The vendor will describe its answer detection methodology.

CenturyLink has read, understands and will comply.

Answer detection is based on the measurement of incoming signal energy on the telephone line. When the called party is instructed to accept or reject the call, the system "listens" for either the appropriate DTMF or the correct count of rotary-dial pulses. The ITS uses answer detection to recognize busy signal, ring no answer, and invalid number announcements (SIT Tones) by listening for specific call progress tones and silence intervals on a call. Answering machines, pagers and voice mail responses will all be treated as incomplete calls. Only a positively accepted call will generate a call charge to the paying party.

3.9.14 The inmate's call will be muted until the called party has positively accepted the call. The ITS will not allow the inmate to hear the called party prior to the actual positive acceptance of the call.

CenturyLink has read, understands and will comply.

This is currently the standard procedure for NDOC. In addition, billing for the call will not begin until the called party had positively accepted the call, which is after all the prompts and information incoming call completed.

3.9.15 The ITS will be capable of limiting the length of a call, providing the dial tone at certain times of the day and allowing a maximum number of minutes per inmate, per month.

CenturyLink has read, understands and will comply.

NDOC's current practice is to not limit the general population to a maximum number of minutes; however, if NDOC wishes to implement these restrictions, CenturyLink will be able to do so.

3.9.16 In all circumstances, the ITS will limit the inmate to a single call request. The ITS will always require the inmate to disconnect and initiate another call.

CenturyLink has read, understands and will comply.

3.9.17 The vendor will provide information on any additional or optional features, investigative or management systems or tools provided that may be of interest to the NDOC (i.e. word recognition/keyword search, reverse look-up, visitation telephone recording, etc.) Please ensure a complete description of the features application is included. Any cost associated with the additional or optional features described shall be included in the vendor's cost response *Attachment P, Cost Commission Proposal.*

CenturyLink has read, understands and will comply.

Value-Added Features

As we move NDOC from the current premise-based system to our state-of-the-art centralized system, CenturyLink is able to offer a number of new value-added features to the Department. In addition, many of these features can only be provided by CenturyLink, given our corporate capabilities, strategic partnerships, and history with NDOC under the current contract.

❖ *UNIQUE CAPABILITIES* ❖

CenturyLink is uniquely positioned to provide a number of value-added features to NDOC, driven by:

- ✓ ***Our exclusive partnership with the Keefe Group, now in the process of installing banking and kiosk services throughout the agency***
- ✓ ***Our knowledge of NDOC given our past 6 years of service under the current contract***
- ✓ ***Our in-place, in-state service resources based in Las Vegas to assist NDOC with any operational or training needs***
- ✓ ***CenturyLink, Inc.'s position as the Incumbent Local Exchange Provider in Southern Nevada***

Offerings are divided into three sections depending on the financial impact to the Department, inmates, or Friends and Family (F&F) members:

Offers with no cost to NDOC, inmates, or friends & family
Offers with no cost to NDOC, but with fees to inmates and/or friends & family
Offers impacting commissions to NDOC or rates to inmates and friends & family

Financial impacts, if any, are detailed in Attachment P.

We look forward to discussing these technologies that will streamline investigations, improve staff efficiency, simplify inmate communications and operations, and increase connections between inmates and their friends/family with the Department.

SUMMARY OF VALUE-ADDED FEATURES

Value-Added Functionality – No Cost to NDOC, Inmates, or Friends & Family			
#	**Feature**	**Description**	**Benefit**
	Operational Tools		
(1)	**Augmentation of Keefe kiosk-based inmate services**	• Replicates kiosk functionality on inmate telephone system ✓ Commissary ordering by phone ✓ Grievance filing, Appointments, inquiries ✓ Staff to inmate communications ***Unique feature through CenturyLink's exclusive partnership with Keefe***	• "Full backup" for EDGE kiosk system • Uses plentiful inmate telephones and avoids lines at kiosks • Complete integration with Keefe systems = information synchronized from single data source
(2)	**Direct Link Trust Debit** ** ***Unique feature through CenturyLink's exclusive partnership with Keefe*** **	• Calls debited from inmate trust account directly. • Interface already built with to-be-installed Keefe/ATG banking system	• Real-time, by-the-call payment drives more calling and commission revenue • No separate debit "account" - drives all debit funding through banking (ensures restitution and other payments are made)
(3)	**Continuation of current attorney verification and audit process** ** ***In place at NDOC today*** **	• Inmates input attorney numbers over inmate telephone system; CenturyLink verifies numbers as belonging to attorneys • Entire attorney list audited quarterly	• Input over phone = no paper request forms + audit trail • Offloads work from NDOC staff • Validates data for non-recorded numbers
(4)	**"The Communicator" Paperless Inmate Communications**	• Part of kiosk replication (#1) above • Two-way communication feature built into Enforcer ITS • Can be used for	• Eliminates paper • Audit trail for inquiries and responses • Staff can respond using text to speech technology, if desired

	** ***Certain modules in place at NDOC today*** **	appointments, grievances, or covert tips • Used today for inmate balance inquiries and "Message of the Day"	
(5)	**Emergency Auto-Dialer**	• Can provide call-outs to numbers called by inmates for facility incidents (general information / all fine notifications) • Can be generated on short notice using ITS call lists • Part of CenturyLink's existing disaster recovery plans	• Reduced staff workload • Better communications with F&F
Security & Investigative Tools			
(6)	**Inmate to Inmate Communications (ICER)**	• Identifies inmate-to-inmate communications	• Alerts automatically identify suspicious activity for investigators
(7)	**Additional Investigative Assistance** **(Includes Access to Additional Reverse Lookup Databases)**	• Exclusive access to additional databases – including carrier subpoena contacts. • Unique carrier relationships drive additional value	• Increased investigative staff efficiency • Ex: recently unlocked cell phone SIM card in murder cold case
(8)	**Data Detective – investigative data across phones, deposit services, e-messaging** ** ***Unique feature through CenturyLink's exclusive partnership with Keefe*** **	• Visual Link Analysis of connections between inmates and called parties • Data include inmate calling AND Keefe group e-messaging and deposit services	• Increased investigative capabilities through visual link analysis and multiple data sources
(9)	**Call pattern analysis**	• Identifies and reports on suspicious calling patterns • Complements visual link analysis tools	• Increased efficiency among investigative staff
(10)	**Officer Check-in**	• Check-ins from officers doing rounds or beginning shifts using phone system	• Database tracking of officer movement
(11)	**PREA reporting + Crime**	• Anonymous tip reporting to	• Part of PREA compliance

	Tips ***** Certain modules in place at NDOC today *****	unlimited number of numbers or mailboxes • Completely configurable for live answer, answer by NDOC voice messaging system, or CTL-provided voice messaging system	efforts • Straightforward reporting and auditing
(12)	**Integration and Data Sharing With Clark County, City of Las Vegas, and Other Correctional Facilities** ***** Unique feature through CenturyLink's existing customer base in Nevada*****	• Access across multiple agencies – privileges can be managed by CenturyLink personnel to offload work from NDOC staff	• New source of investigative data • Ability to navigate systems without re-training efforts • Increased efficiency among investigative staff
Service Capabilities & Commitments			
(13)	**Backup Technical Assistance from CenturyLink, Inc.** ***** Unique CenturyLink capability*****	• Ability to call on higher-level technical resources (e.g. fiber cable locators/splicers) for special maintenance situations	• Faster resolution of potential service issues
(14)	**Cross-Training of ITS technicians on kiosk solution**	• CenturyLink technicians will be cross-trained to maintain the Keefe kiosks	• Improved service and uptime for inmate kiosks
(15)	**Additional bandwidth**	• Additional network bandwidth available through CenturyLink, Inc.	• Additional cost savings to the Department
(16)	**Quarterly Service Reviews** ***** In place at NDOC today *****	• Consultation on new products & features, legal & regulatory issues	• Ongoing knowledge of options available to the Department

Value-Added Functionality – No Cost to NDOC; Funded by Inmate or Friends & Family Fees			
	Feature	**Description**	**Benefits**
(17)	**Video Visitation**	• Offered as pilot program; expansion at NDOC's discretion • Skype-like capability	• Reduced staff involvement • Additional communication channel to F&F

(18)	**Inmate Voicemail** ** ***In place at NDOC today*** **	• Standard inbound voicemail from family members to inmates, maintaining security controls.	• Increased communication with family • Revenue source

Value-Added Functionality – Impacts Commission and/or Calling Rate Offers to NDOC			
	Feature	**Description**	**Benefits**
(19)	**Voice Biometrics (pre-call verification)** ** ***In place at NDOC today*** ** ** ***Can be continued without need to re-enroll inmate population (CenturyLink exclusive)*** **	• Matches inmate voice with PIN prior to allowing call to be made	• Reduces PIN theft • Can be continued without need to re-enroll inmates
(20)	**Voice Biometrics – Investigator Pro (continuous verification)** ** ***In place at NDOC today*** ** ** ***Can be continued without need to re-enroll inmate population (CenturyLink exclusive)*** **	• Analyzes inmate and called party voices continuously throughout call • Identifies impostors and other suspicious activities	• Reduces PIN theft • Identifies inmates trying to hide identity over phone system
(21)	**Recorded visitation phones**	• Place ITS security features on visitation phones – e.g. PINs, recording, voice biometric authentication	• Automated monitoring of visitation phones
(22)	**Cell phone detection options**	• Variety of methods available – refer to response to 3.11.1.5.	• Detect & prevent contraband cell phones
(23)	**PREA Pro™ Reporting Tool**	• Detailed reporting, event management, and case management tool for PREA administration	• Assists Department by automating reporting and auditing for PREA compliance
(24)	**Location of called cell phones / "geo fencing"**	• Ability to locate called cell phones and place "geo fence" perimeter around correctional facilities	• Facility security