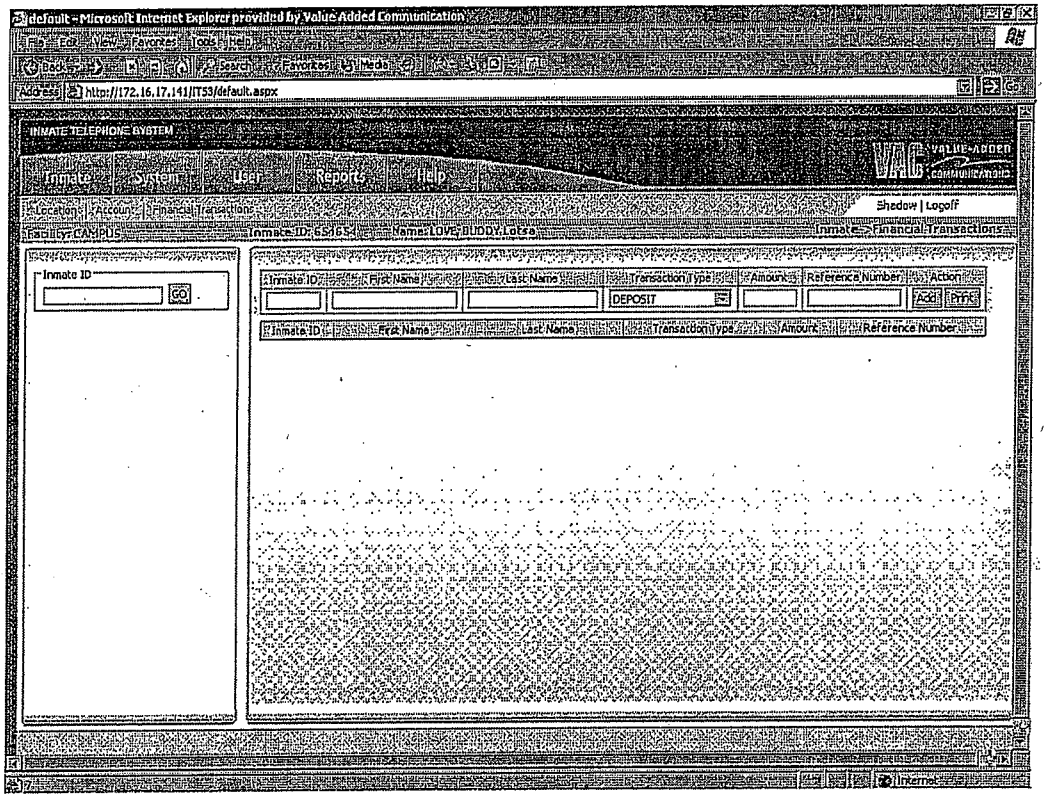
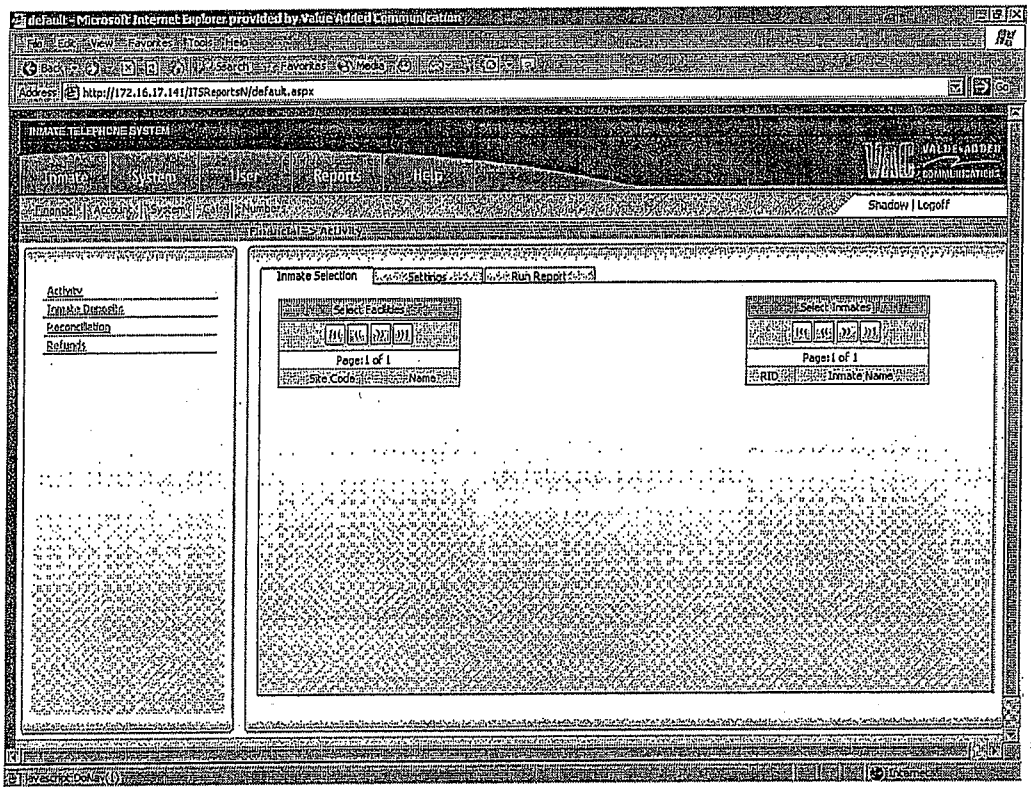
To accomplish the above tasks, the FOCUS 100 workstation will be able to use the user friendly web application to make manual adjustments to the Inmate PrePaid account. An audit trail is maintained to allow for easy reconciliation of accounts.





4. Attachment 10 is the DOC Policy number DC-ADM 818-1, date of issue August 19, 2004 with effective date September 19, 2004 for prepaid phone card refunds. The Contractor shall explain how the prepaid phone card refund requirement shall function. The Contractor shall explain prior experience with inmate prepaid services including locations, length of experience, and scope of services all to be included in the proposal. The system will be required to calculate the cost of each phone call based on the rates. The contactor shall describe how the system proposed rates phone calls and charges them to inmate accounts. The Contractor shall describe how to handle inmate accounts from going into a negative balance. Monthly minimally prepaid reports will be similar to the current summary prepaid reports in Attachment 22.

MCI Response:

MCI has read, understands and will comply.

MCI will support the DOC Policy number DC-AMD 818-1 with an issue date of August 19, 2004 and effective date of September 19, 2004.

With regard to the process to issue a PrePaid Phone Card to an inmate upon release, MCI will follow the process described in RFP Attachment 10. The MCI Commonwealth Manager will manage the process and work with the Commonwealth to insure that all reporting and administrative requirements of DC-AMD 818-1 are met.

For the PrePaid Card System, MCI proposes VAC's PrePaid Card service. The service works in conjunction with VAC's V-Connect Service as also proposed by MCI to meet the direct billing requirements of this RFP.

VAC's PrePaid Card service is an establish service operational today for use by VAC's existing customer base. The service has been in use and available

The system will calculate costs for the call based upon a charged rate. Because the PrePaid Cards and non-rechargeable the account can not go into a negative balance.

MCI will support any and all monthly Prepaid Card reports.

5. Prepaid Calling Services is an alternative calling method that allows inmates, family and friends to pay for the inmate's telephone calls by using funds in the DOC-SCI commissary account to create a telephone debit account. The inmates move money from their commissary account to a telephone account through the commissary transaction process. The DCRMS offers the inmate the opportunity to make a collect call or a prepaid call through its call control platform installed at all DOC-SCIs. When an inmate chooses to make a prepaid call, the call accesses the T-Netix (Securus Technologies) prepaid server to determine the balance in the account. If there is enough money in the account to make a one (1) minute call to the dialed number, the call is allowed to proceed. The cost of this call is deducted from the inmate's telephone account. At any time the inmate may check the availability of prepaid funds in his or her prepaid account. In general, the inmates go to the commissary once a week and may purchase prepaid time in amounts of $15.00, $25.00, $50.00. Effective May 17, 2004, the amount of prepaid time an inmate is allowed to purchase per week increased from $50.00 to $100.00. These three (3) prepaid amounts are not likely to change, but may. The Inmate prepaid account is currently averaging a nine (9) percent discount, which includes appropriate taxes, but does not include the State six (6) percent tax which is paid by the inmate when he or she purchases his or her prepaid account from a DOC-SCI commissary. Prepaid calling services are used at all DOC-SCIs and would be used in any new DOC-SCI facilities. All DOC-SCI commissary systems are under the DOC Bureau of Correction Industries personnel with the exception of SCI Pine Grove which is currently contracted with Keefe Communications Networks.

MCI Response:

MCI has read, understands and has proposed an equivalent PrePaid Solution in response to this RFP.

6. The central processor shall have the following functionality:

- Monitors all traffic at SCIs
- Get real time reports from SCIs Backup SCI if SCI goes down. May not apply to a centralized system, however Contractors are to describe both centralized and decentralized in technical requirements and these reports are required in decentralized.
- Provide real time status of all SCIs
- Redundancy (duplicate)
- Collect data from each telephone call immediately after completion of call

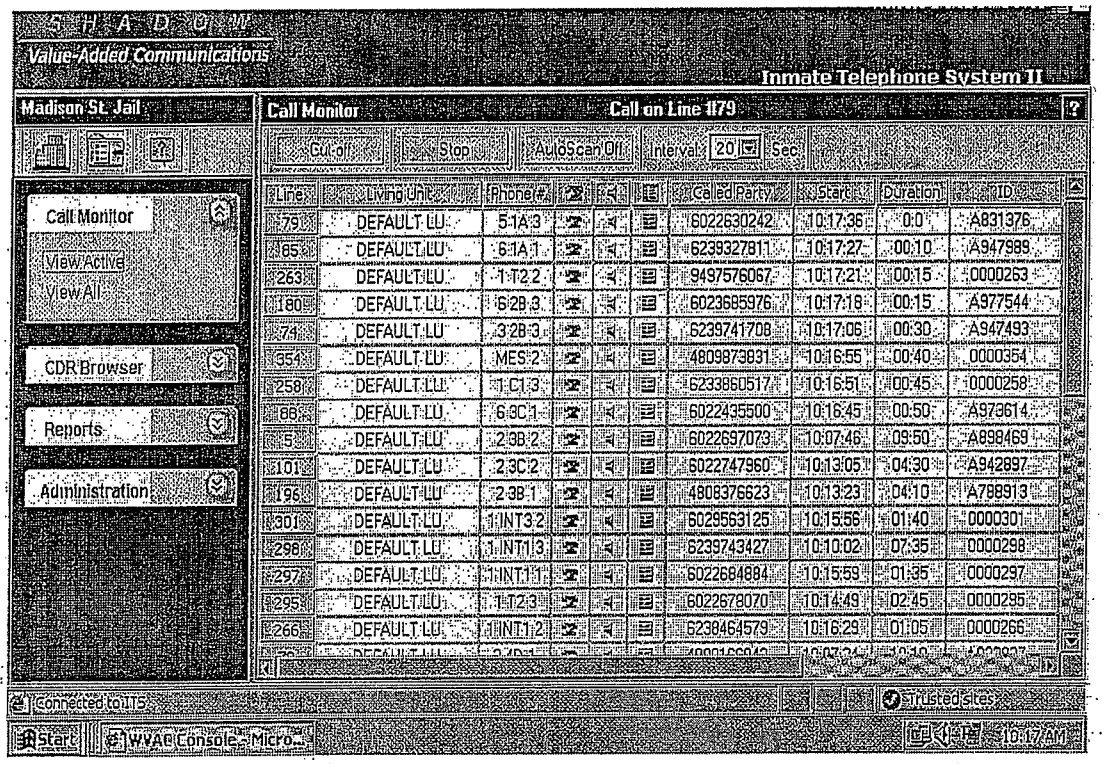
- Store data in a relational database or equivalent
- Four (4) hour power supply backup.
- All information shall be separated by each facility. For example, if a Contractor chooses to use a centralized computer or controller, all information must be partitioned by facility.

MCI Response:

MCI has read, understands and has complied with a system that will meet each of the above requirements.

[redacted]

A feature which most other vendors do not offer, the investigator may [redacted] What a great utility that allows [redacted] is to monitor all calls in progress, allows the user or monitor to perform other important duties or tasks. [redacted]



Live Monitor / Auto Scroll

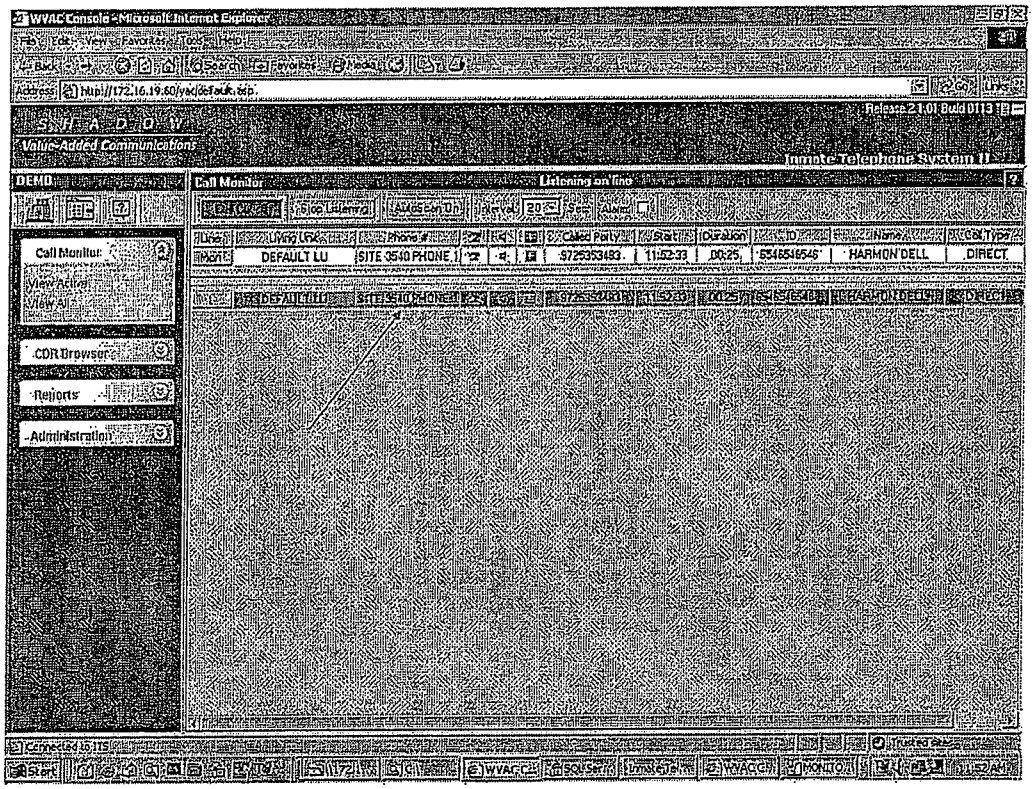
Alerts can be set through the workstation for either a specific inmate PIN or a specific called number which would automatically initiate a visual notification to investigators that an alerted call is in progress and call monitoring could begin immediately.

Digital Spy Silent Monitoring Capability

Investigators with the appropriate access level may silently monitor calls in progress using the Spy function of the Focus 100. Monitoring can be specific to an individual facility, or with the appropriate security clearance or access level, they can monitor ANY facility within the DOC by means of the secured WAN / VPN (Wide Area Network / Virtual Private Network) that is provided by MCI. The investigator can view calls in progress, select the one to monitor and begin listening in a matter of seconds. Monitoring remote facilities functions exactly the same ass if the workstation was physically attached to the on-site server.

These advanced monitoring capabilities with digital quality are a standard feature of the Focus 100 ITS. With the years of experience that both MCI and VAC have in the inmate telephone system business, we have determined that you can not provide enough investigative features, but the auto scrolling feature is one that goes above and beyond the call of duty.

Whether remote or locally attached to the ITS, the workstation user while listening to a call can disconnect that call in progress by simply clicking the mouse on the [CUT CALL] button as shown below in the example provided.



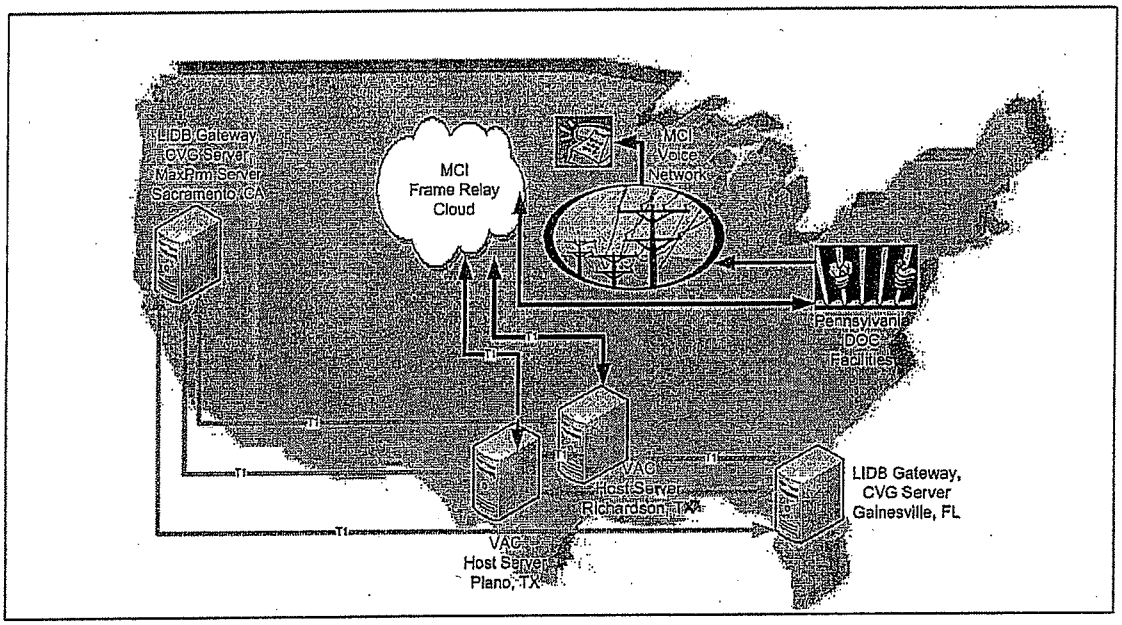
Live Monitor / Call in Progress

Real-time reports are always available regardless the system type, B or C and regardless if the on-site ITS is online or not, because of the uniqueness of the Focus 100 platform. Reports are generated by querying Call Detail Records (CDR). CDRs are stored redundantly, onsite, at the VAC headquarters in Plan, TX, VAC's backup redundant location in Richardson, TX. And if that isn't enough, MCI additionally stores the CDRs in our Sacramento, CA system development center. The workstation is not dedicated to the uptime of the local server or a centralized server. When performing a report query or print request, the system will follow the necessary network path to gather the information requested, thus always providing for Real-Time reports.

As detailed in earlier sections, the data (CDR) from each telephone call is captured immediately on the local RAID hard drive in redundant locations, and is also stored in 3 other physical locations for thorough redundancy. This data is stored for 7 years after the end of the contract. Shown below is a Commonwealth Map depicting the redundancy of data captured and stored. All information is stored independently and identified by facility. The use of on-premise equipment allows for the easy identification of specific facility data.

Each facility will be provided with a 4 hour UPS to allow for the Focus 100 to operate for 4 hours in the event of power failure. At a considerable expense and a reduction in

commissions, the 4 hour UPS will continue to power the Focus 100 system while the entire facility may be without power. It has been the experience of MCI that a 1 hour UPS is sufficient in the event of power outages, since the facility is usually in a lockdown situation with a facility power outage. But as a requirement of this RFP, MCI is willing to comply and offer large 4 hour UPS / Backup Power sources.



As detail in section 2.5-A.1.e, the site monitoring application is a value-added feature that MCI is offering to the Commonwealth at no additional cost which provides real-time status as required in this section. MCI will provide access to this tool and data to a limited number of DOC and Headquarters staff. Upon request for this feature, MCI will work with DOC representatives and site personnel to implement the feature and provide the necessary training to DOC staff.

The Site Monitor tool is a revolutionary method for monitoring the health of the entire ICS solution from a frame relay wide area network (WAN) connection to the ICS platform. It communicates with each system every 15 minutes to verify that the platform and network are fully operational. Thus, it will notify MCI on a near-real-time basis of any suspected service-impacting event, enabling MCI to begin problem resolution before facility staff become aware of the problem.

In addition to checking the health of the system every 15 minutes, the Site Monitor application performs the following tests and checks:

- **IPing.** Site Monitor will proactively "ping" the Cisco IP router and ICS server located at each DOC site to verify network connectivity to the facility systems and that they are active. MCI will immediately take steps to resolve the problem before it is evident to facility personnel.

- **Call Failures.** Once per hour the Site Monitor will calculate the number of failed call attempts against the total number of attempts—unbillable and/or failed vs. completed billable calls. When a high failure rate is detected, the system will automatically generate an alarm, prompting the MCI Service Center and Network Operations Center to troubleshoot the problem and begin appropriate resolution activities.

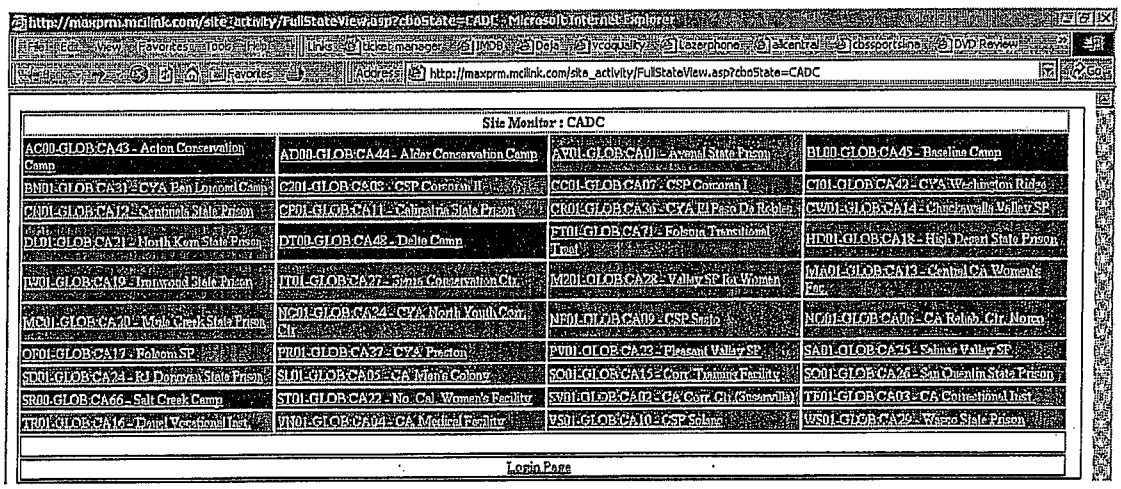
- **Call Blocks.** Once per hour the Site Monitor will calculate the number of blocked calls against the number of completed or billable attempts. If a high block rate is detected, the system will automatically generate an alarm that prompts MCI's investigation and resolution activities.

- **Billable Calls.** Once per hour the Site Monitor will compare each facility's number of billable calls against historical volume for the same day and time period (e.g., the past three Tuesdays for the one-hour time period of 5:00 PM to 6:00 PM CDT) to identify aberrations in call volume. This process helps identify possible service-impacting events. For example, a site that shows a zero usage traffic volume could indicate the occurrence of a major outage or simply that the site is in lockdown or delayed inmate count status.

MCI's Site Monitor tool is an intelligent device that can monitor multiple, geographically diverse locations, each with unique features, resolution time frames and calling parameters. The functions of MCI's Site Monitor are performed from MCI's development facilities in Sacramento, CA. By maintaining a physically diverse location for monitoring, MCI can initiate trouble tickets even if the entire Commonwealth is without service. Another benefit of placing the Site Monitor functions in Sacramento is that MCI's DOC Account Team can leverage its internal on-site development resources and implement programming enhancements to the system.

Identifying potential service-impacting events is the first step of proactive monitoring, and alerting key staff to these events is second. Once an event is identified, key MCI Account Team personal, field operations personnel, and the Service Center staff are sent a text page as well as a priority email alerting them of the event. If requested, MCI can also ensure that DOC personal are notified.

The image below depicts the MCI Site Monitor tool's screen shot of an entire Commonwealth overview. Red would indicate a potential service-affecting issue worthy of investigation. Yellow indicates that a red issue has occurred and is in the problem resolution process. Blue indicates all is well and normal. Black indicates the absence of site traffic.



Site Monitor Report / State View

7) The SCI control processor or device shall have the following functionality:

- Provide control for inmate call control system
- Collect call data - two (2) calendar days capacity
- Produce reports in real time in coordination with the central processor
- Four (4) hour power supply backup.

MCI Response:

MCI has read, understands and will comply.

MCI will install a state-of-the-art fully automated inmate call management system to meet the specific needs of the Commonwealth. This CPU based system is based on proven telephony technology, designed specifically to operate with the highest degree of reliability in the challenging environment of a correctional setting. VAC developed the proposed system on a foundation of accurate, reliable call processing – followed by the integration of an extensive array of call management features and investigative tools unparalleled in this industry.

As specified, the proposed system will provide inmate specific controls using a Personal Identification Number for each inmate. Each inmate PIN account can be further managed through the use of a limited allowed call list, call duration control, calling hours control, and defined phone access. Each and every call attempted through the system generates a call detail record. The collect call data is stored for the life of the contract on each on-premise and centralized servers. Redundant copies are also stored on different servers in different locations. Thus, the 2 day requirement for capacity of the collect call data is met with the lifespan of the contract plus an additional 7 years commitment.

This record is the cornerstone to the system's investigative capabilities. The Focus 100 ITS offers a variety of means to search call records (CDRs) by inmate, called number,

date, time, or inmate phone. Harassing phone calls can be quickly isolated and the offender identified using CDR data. In addition, each call will be digitally recorded using VAC's Shadow technology. Through that same CDR, the investigator may quickly retrieve and play the recorded conversation. All reports from the Focus 100 ITS are in real-time in coordination with the central processor or on-premise processor.

MCI will provide the Focus 100 Call processing technology along with the required investigative and call control features specified by the CUSTOMER. MCI's team of seasoned professionals will install and test the system and will provide training to appropriate facility personnel. In addition, MCI will provide both remote and local technical support to the DOC as needed throughout the project duration. And as detailed in the previous section, MCI will provide the 4 hour battery backup / UPS system for the Focus 100 system.

p. System Administration:

1. Contractors shall respond to this requirement of the RFP with two options for consideration and decision by the Commonwealth.

a. Option 1 - A central processor in coordination with location processors supported by a decentralized staff of system administrators serving each SCI, the Quehanna Boot Camp, and the terminals at the Headquarters Security and Professional Responsibility Offices. Refer to 2.5-A. 2.p. (1) a. Option 1.

MCI Response:

MCI has read, understands and has complied with the cost options in MCI's financial response of this RFP.

b. Option 2 - A central processor in coordination with location processors or system control devices at all SCIs, supported by a centrally located system administrator(s) controlling the inmate telephone service, and the terminals at the DOC Headquarters Security Office, the Headquarters Office of Professional Responsibility. Refer to 2.5-A. 2.p. (1). b. Option 2.

Paragraph p. refers to two (2) options. These options are for decentralized and centralized administration. The decentralized option, as used presently, requires administrators at each SCI versus administrators only at the centralized site. There will be administrative costs in people and possibly costs in data processing equipment associated with either approach in meeting the requirements for central processor functionality and SCI central processor functionality. The intent is that the central processor in coordination with the SCI processor shall meet the functionality for either the decentralized administration approach or centralized administration approach. The details of the coordination effort may vary in that they may entail various degrees of manual and/or automated procedures. However, in all case, the user functionality must remain essentially the same. The procedures and associated processing requirements on the central and SCI processors may vary but functionality must be maintained. The Contractor may split the coordination function any way it deems right for it, but the user function must remain constant. Automation of data entry of inmate PIN numbers into the inmate calling system by using bubble sheet scanners and other technologies are acceptable to maximize efficiencies in the process.

MCI Response:

MCI has read, understands, acknowledges and agrees.

The System Administration does remain the same for both Option 1, Option 2 and System B as well as System C and any mixture thereof. MCI is furthermore offering to automate a majority of the data entry of inmate PINS as discussed earlier in section 2.5-A System B 1.e Other Features. A brief recap is provided below showing how MCI's NCC assists in the centralization of PIN administration.

Automated Inmate Data Exchange Program (NCC)

In order to streamline the PIN assignment process, MCI is also willing to offer the Commonwealth an automated process by which the Commonwealth can send a PIN information file electronically (XML File Format) to MCI in the appropriate data exchange format. Depending on the method selected by the Commonwealth, implementing the NCC automated function of PINs could be completed within 30 to 60 days if the Commonwealth desires. The Focus 100 system in conjunction with our NCC (Network Control Center) system will provide PIN account creation, updating, and random automatic PIN numbering if DOC so desires. All PIN assignments will comply with DOC policies and procedures.

NCC would provide a mechanism for the Commonwealth to submit an agreeable source of data for processing by MCI. MCI would provide feedback on any problems to DOC regarding any issues with the creation or updating of inmate PINS. The data exchange would be handled by NCC through the use of an FTP server as the transport mechanism to accept a full-dump of PIN data reporting from DOC on a daily bases, or at other predetermined intervals.

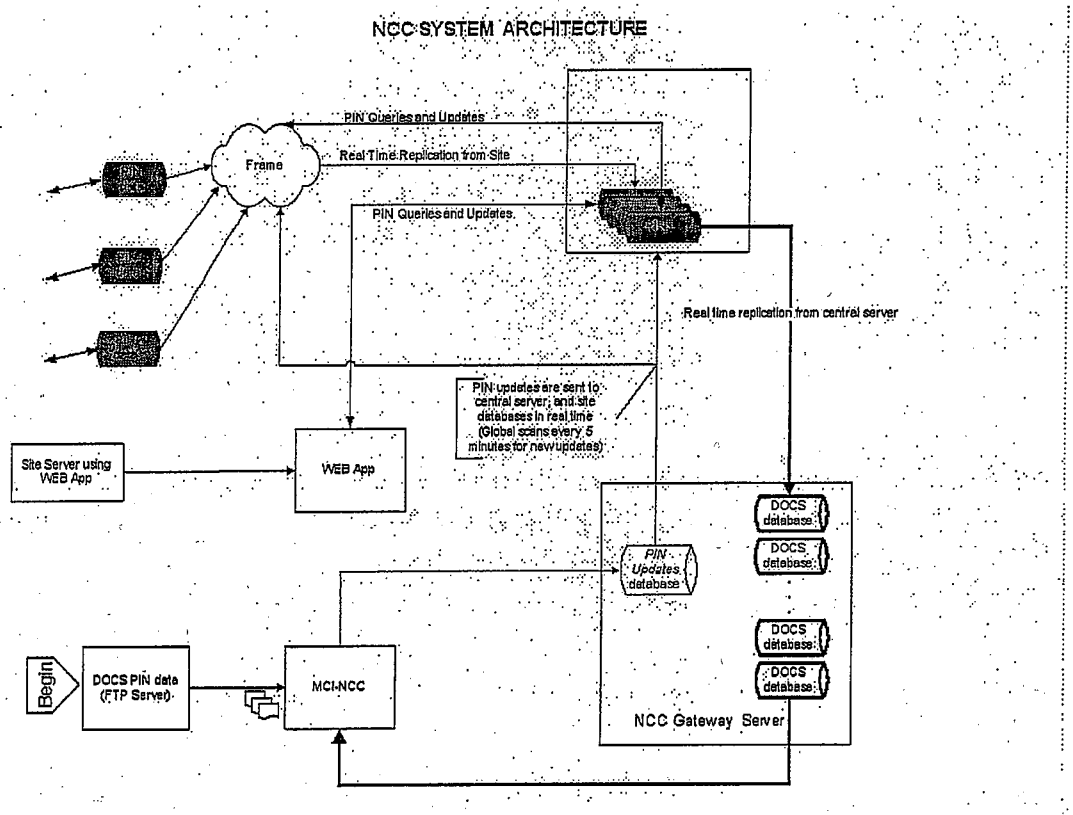
The MCI NCC system comprises of three main players, namely DOC, MCI MAXSEC, and VAC. The role of each player is explained below:

- DOC uploads PIN data files to the FTP server.
- MAXSEC is MCI's PIN support organization and systems. MAXSEC downloads PIN data files from the FTP server, determines PIN changes, and sends PIN changes to VAC.
- VAC updates ITS databases and configures inmate call privileges.

Depending on DOC requirements, MAXSEC will send to VAC a batch of PIN changes, at a frequency of once a day. VAC will check for PIN changes every 5 minutes. PIN changes sent by MAXSEC will be updated on the ITS immediately. Additional detail relating to the NCC process is below:

- DOC uploads PIN data to FTP server (at an agreed upon frequency).
- MAXSEC downloads PIN data and creates PIN changes (adds, edits, and deletes).
- MAXSEC sends PIN changes to the NCC gateway server by inserting PIN update records into a table in the update database located on the NCC gateway server.

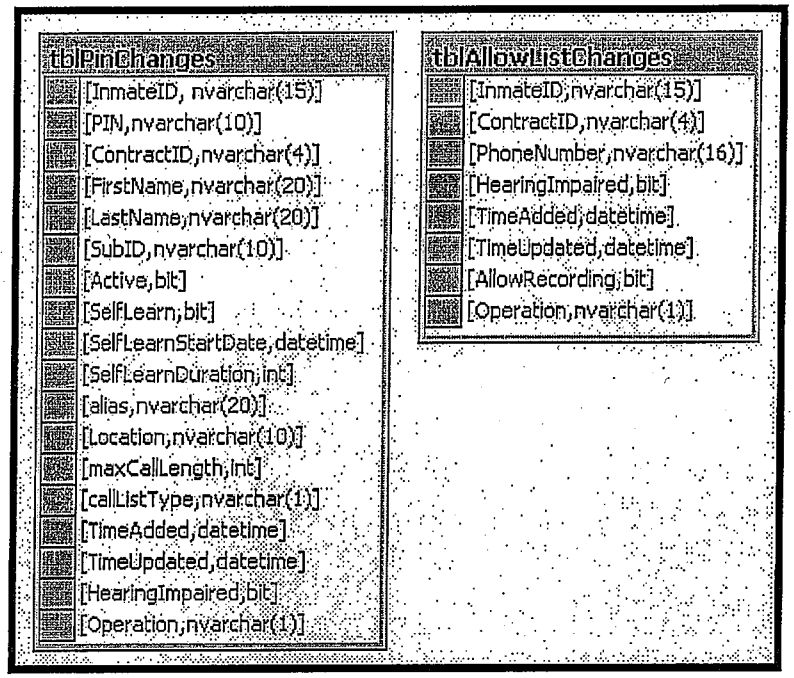
- VAC scans the update database every 5 minutes for new update records. For each new update record, VAC updates the site data using the update record and flags the update record.
- VAC does real time replication of site data to the NCC gateway server. Inmate database is replicated at both the Plano, TX cluster servers and on the VAC Richardson, TX cluster servers to ensure for a fault tolerant PIN administration system.
- MAXSEC runs queries against the NCC gateway server. Because VAC does real time replication of the site data to the NCC gateway server, the data accessed by MAXSEC is the same as the site data.



Network Control Center Architecture

PIN Update Database

The PIN update database (PinUpdates) contains two tables that hold changes in pin data. They are the tblPinChanges and tblAllowListChanges. They are shown below with their sizes and MS SQL data types.



PIN Database Table

There are three kinds of updates, Add, Edit, and Delete. For each add or edit record, the fields to be updated will contain non-null values. All fields that contain null values in an add or edit record must be ignored. Delete records will typically contain fields InmateID and ContractID only.

PIN Updates

The pin update record specifies the data to be modified and the operation field indicates what type of update to perform. If the operation field value is U (update or edit) or D (delete), the ContractID and InmateID field combination serve as a unique key to identify which record is to be updated or deleted. When an update is processed, the update record must be time stamped in the TimeUpdated field.

2. The commission data for each option 1 and 2 shall be entered as required on Attachment 25.

MCI Response:

MCI has read, understands and has complied in MCI's financial response to this RFP.

3. For each option 1 and 2, the system shall be capable of reporting, and notifying the monitoring system operator in real time, occasions when inmate calls placed from different or the same SCI are being dialed to common numbers. The monitoring system operator will be a DOC employee and, in all cases, will be located within the institution. State law prohibits non-Commonwealth personnel access to the monitoring/recording system or its output.